



User Manual

D-Link Central WifiManager

Table Of Contents

Product Overview	3	Monitor	67
System Requirements	3	Report	67
Software Installation	4	Association	67
Central WifiManager Server Installation	5	By Access Point	67
Central WifiManager Server Installation	6	By Wireless Station	68
Access Point Module Installation	9	By Station Number	69
Central WifiManager Server Application	11	Security	70
Access Point Installation Tool	13	Chart	70
Access Point Installation Tool	14	List	71
Central WifiManager Configuration	18	Channel	72
Home	19	Rogue AP	73
Dashboard	19	New AP	73
Site	20	Rogue AP	77
Device View	20	Valid AP	78
Topology View	21	Neighbor AP	79
Configuration	23	SysLog	80
Site	23	Monitor	81
Create Site	24	Monitor Manager	81
Network	26	Create Profile	82
Create Network	27	Monitor List	83
SSID	29	Event	85
Create SSID	30	Type	85
VLAN	47	Standard	85
Bandwidth Optimization	51	Event	86
RF optimization	52	Notice	87
Device Settings	53	Private	88
Upload Configuration	55	Event	89
Firmware Upgrade	56	Notice	90
Undefined AP	58	Condition	91
System	59	Condition Manager	91
Settings	59	Create Condition	92
General	59	Condition List	95
Module	60	Condition List	96
Database	61	About	97
Advanced	63	Appendix A - Front Desk Staff & User Access	98
SMTP	64	Appendix B - How to customize Captive Portal Login Page	108
User Manager	65		
Create User Account	66		

Product Overview

The D-Link Central WifiManager is a versatile, convenient software solution for administrators to manage wireless devices throughout the network from a central point.

System Requirements

For the best results, the following minimum requirements are recommended on the computer used to run the Central WifiManager Server application:

- Hardware:
 - CPU: Intel Core i5 3.2GHz.
 - RAM: 4Gb DDR3.
 - HDD Space: 2 Terrabytes.
 - Display Card: Windows Graphics Card.
 - Installed Gigabit Network Adapter.
- Operating System:
 - Microsoft® Windows 7 (Ultimate/Enterprise) (x86/x64).
 - Microsoft® Windows Server 2008 (R2 with SP2) (x64).
 - Microsoft® Windows Server 2012 (R2) (x64).

Software Installation

In the following section, we'll discuss the software that needs to be installed and used to successfully run the Central WifiManager application.

The following software applications must be installed in order:

- The **Central WifiManager Server** application. This is the main application that will be responsible for day-to-day wireless network management and maintenance. For more information, refer to "**Central WifiManager Server Installation**" on page 5 and "**Central WifiManager Configuration**" on page 18.
- The **Access Point Module** software for all access points that will be used in the Central WifiManager Server application. Every access point has its own access point module software that can be installed on the computer that hosts the Central WifiManager Server application. These modules allow seamless communication between the server and the access points using the Simple Network Management Protocol (SNMP). For more information, refer to "**Access Point Module Installation**" on page 9.
- The **Access Point Installation Tool**. This utility can be used to find new access points on the network, change the IP address of each access point, and upload the network data file for each access point. For more information, refer to "**Access Point Installation Tool**" on page 13.

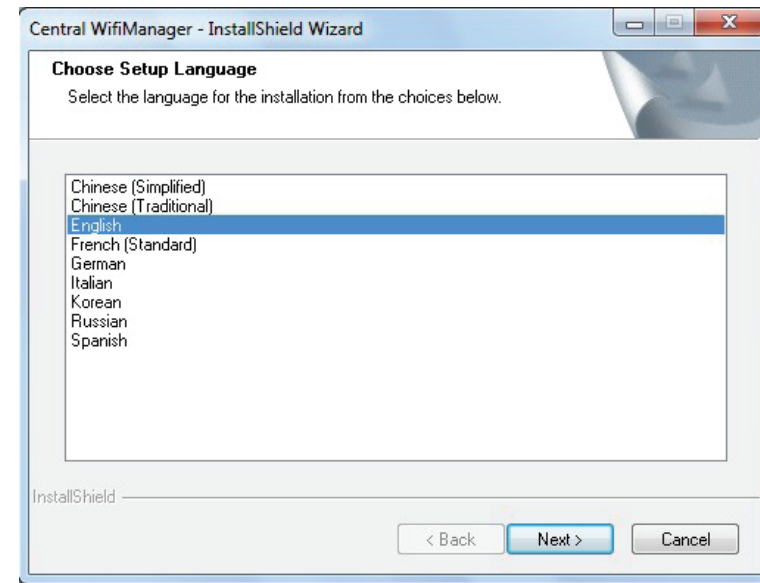
Included at the end of this document, we have the following appendices with additional information that can be helpful to the reader:

- "**Appendix A - Front Desk Staff & User Access**" on page 98.

Software Installation Central WifiManager Server Installation

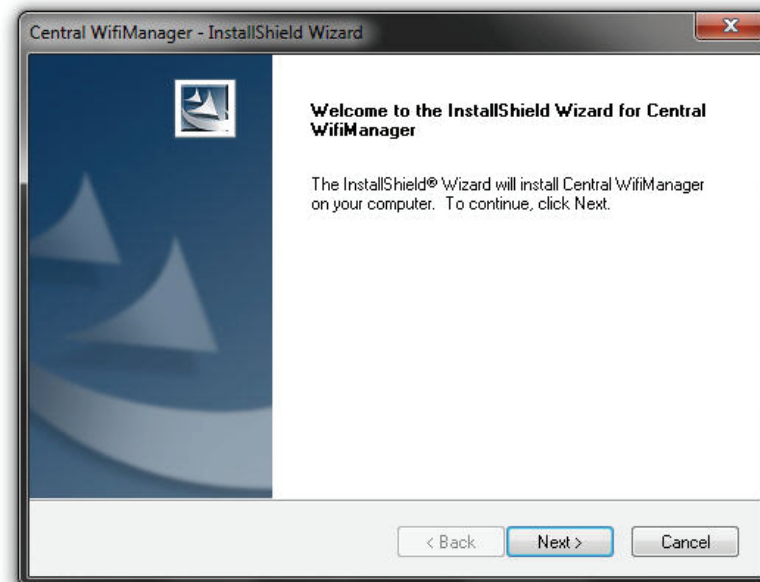
In this section, we'll discuss the installation procedure for the D-Link Central WifiManager software. After running the installation file, a language select window will be displayed for choice.

Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



In this window, a welcome window will be displayed.

Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.

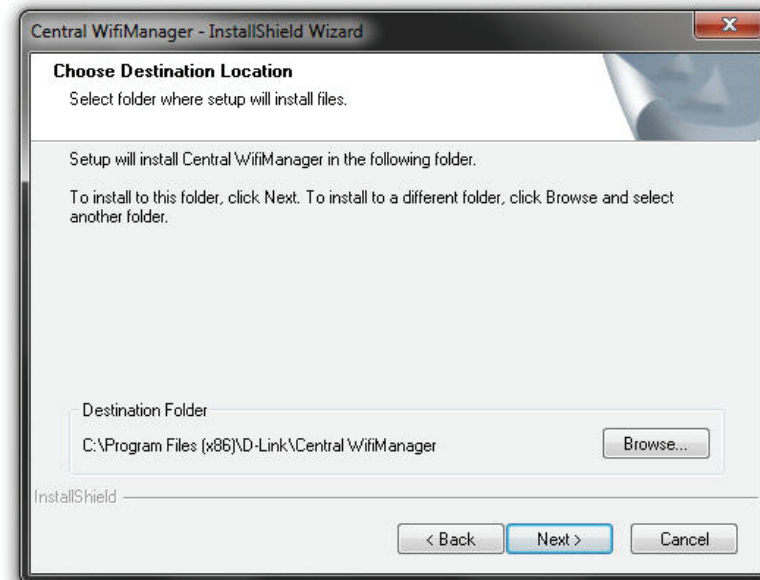


Software Installation

Central WifiManager Server Installation

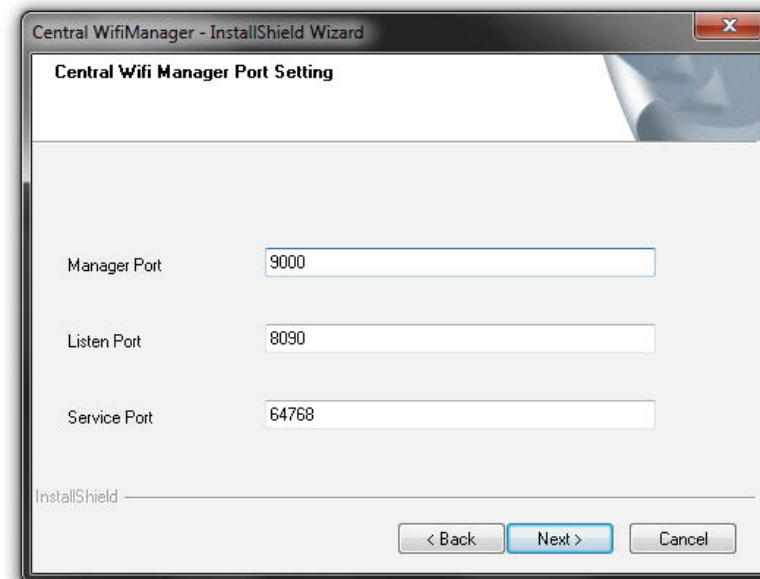
In this window, the destination location is displayed, where the software will be installed. If this application needs to be installed at a different location or on a different drive, click the **Browse** button and navigate to the new destination location.

Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



In this window, we can view or modify the **Manager**, **Listen** and **Service Port** numbers.

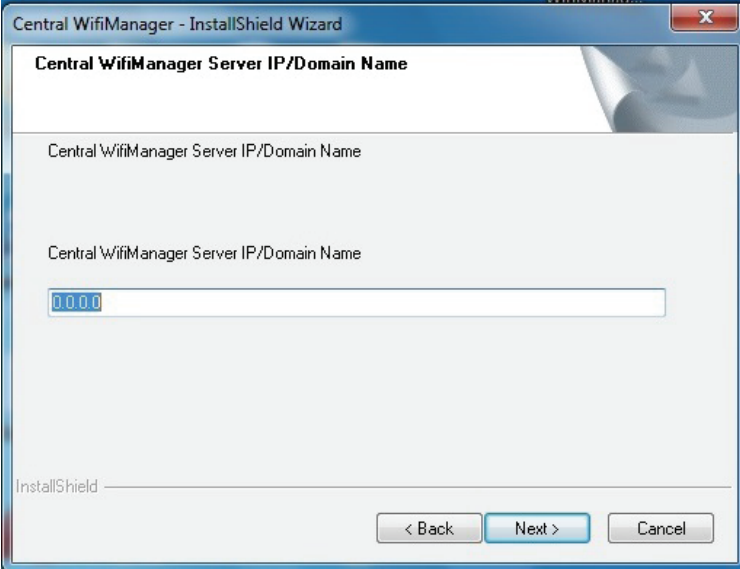
Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



Software Installation Central WifiManager Server Installation

In this window, we need to enter the IP address or Domain Name for the Central WifiManager in the **Central WifiManager Server** space provided. This is normally the IP address of the PC being used for the installation.

Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



Central WifiManager - InstallShield Wizard

Central WifiManager Server IP/Domain Name

Central WifiManager Server IP/Domain Name

Central WifiManager Server IP/Domain Name

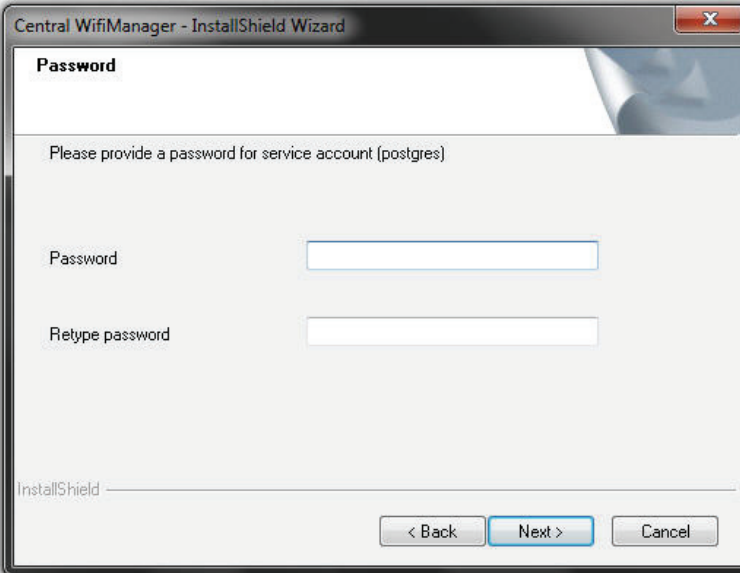
0.0.0.0

InstallShield

< Back Next > Cancel

In this window, we must enter the PostgreSQL password that will be associated with this application in the spaces provided. Enter the same password in the **Password** and **Retype password** spaces provided.

Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



Central WifiManager - InstallShield Wizard

Password

Please provide a password for service account (postgres)

Password

Retype password

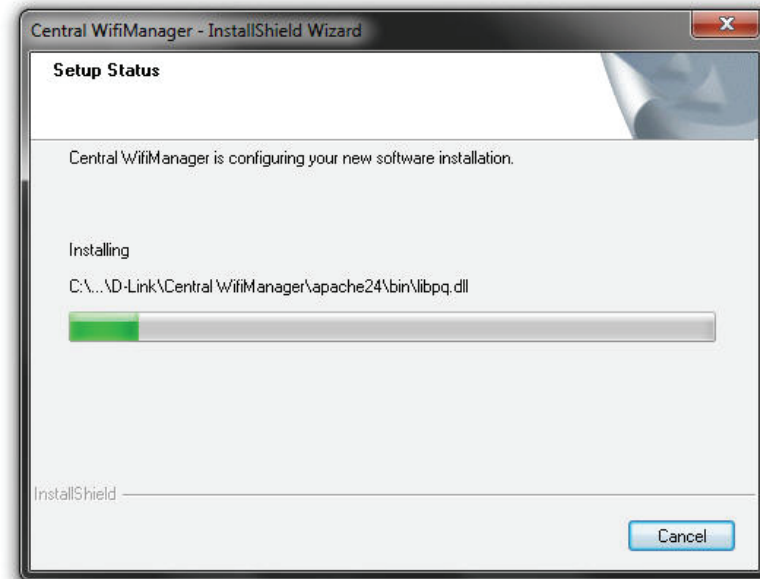
InstallShield

< Back Next > Cancel

Software Installation Central WifiManager Server Installation

The Central WifiManager software installation is running.

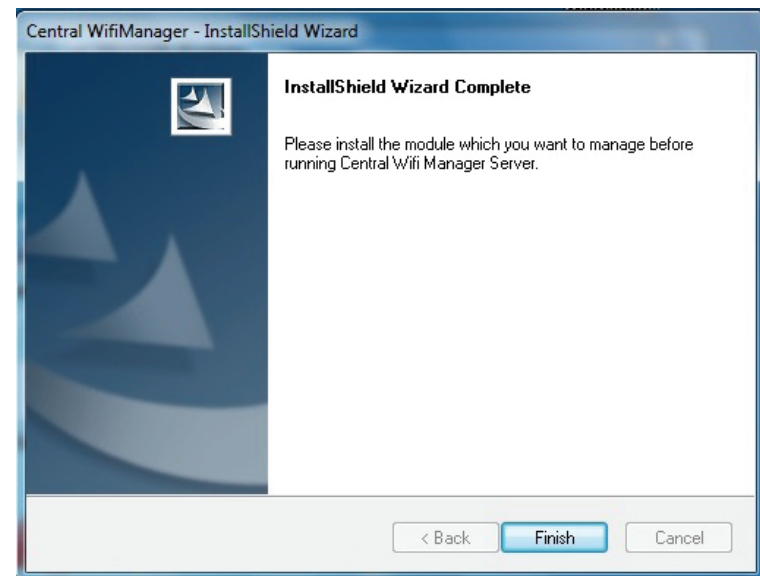
Click the **Cancel** button to stop and exit the installation.



The Apache HTTPS Server application might be blocked by the computer's firewall. If Windows' default firewall is used, a security alert message will be displayed. Click the **Allow Access** button to allow this application to communicate with the network.

In this window, the user is reminded that apart from the Central WifiManager installation, each access point that will be used in this application requires a separate module to be installed. This will be discussed in the next section.

Click the **Finish** button to complete and exit the installation wizard.



Software Installation Access Point Module Installation

For each access point that will be used in the D-Link Central WifiManager, we need to install an additional manager module. In this section we'll discuss the installation of the DAP-2330AP access point's manager module that will be used in the D-Link Central WifiManager.

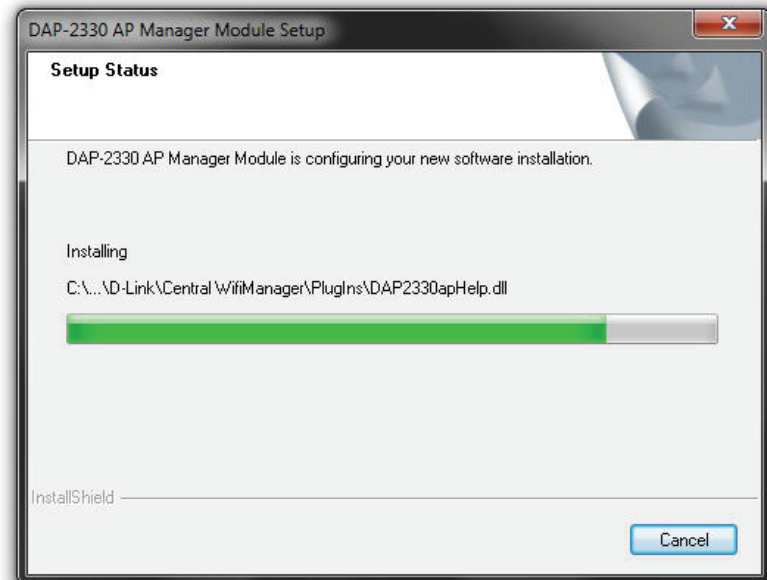
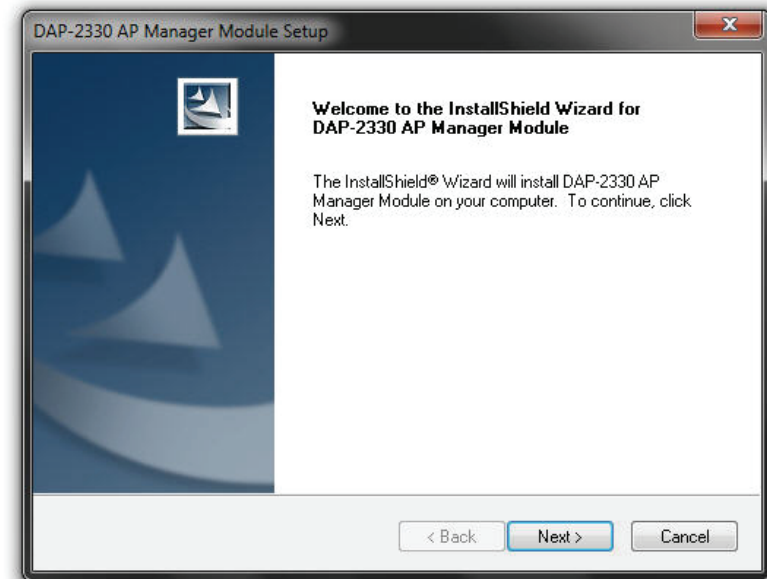
NOTE: If the Central WifiManager Server is already running, it must be stopped and closed before that Access Point manager module can be installed.

After running the access point's manager module, a welcome message will be displayed to inform the user that the manager module will now be installed on the computer.

Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.

After clicking next in the previous step the access point's manager module will be installed.

Click the **Cancel** button to stop and exit the installation.

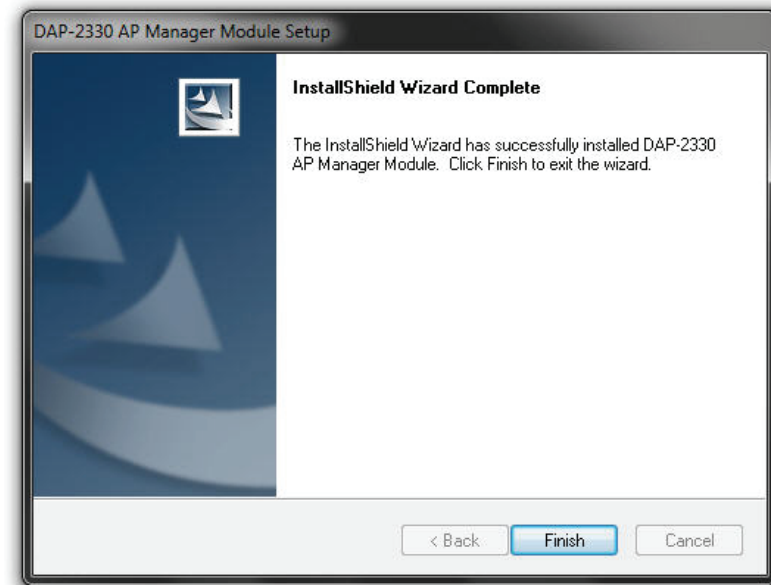


Software Installation

Access Point Module Installation

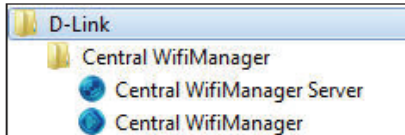
After the access point's manager module was installed successfully, this window will appear.

Click the **Finish** button to complete and exit the installation wizard.



Software Installation Central WifiManager Server Application

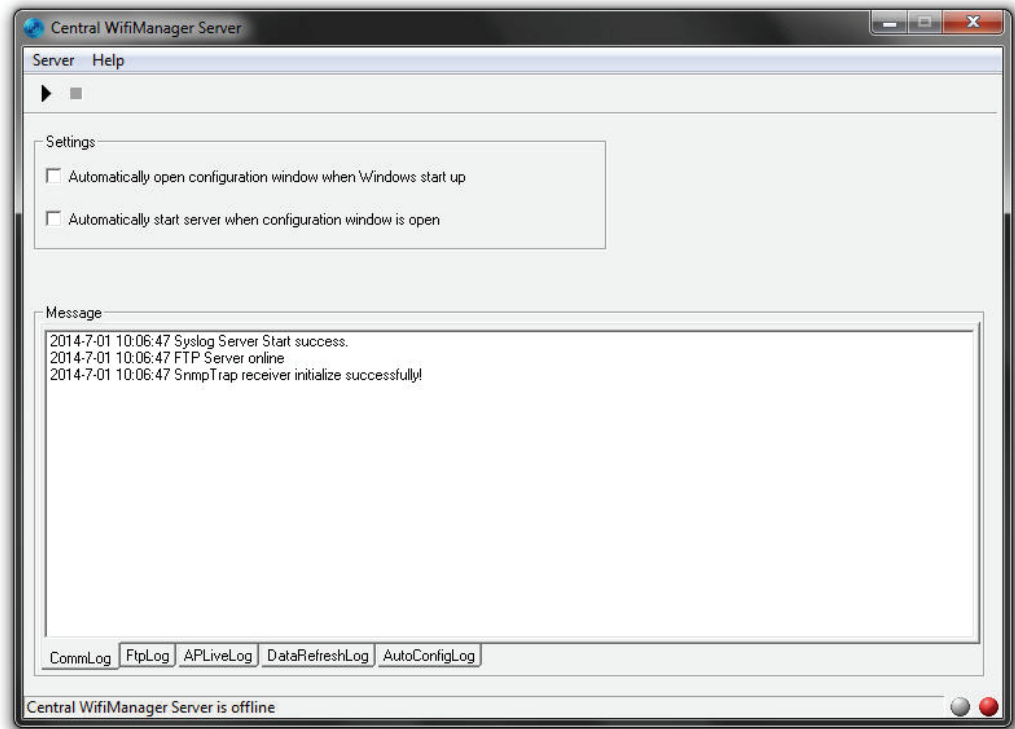
In this section, we'll discuss the Central WifiManager Server application. After the installation was completed the following applications will be available.



Click the **Central WifiManager Server** option to open the server application.

After running the Central WifiManager Server application, the window (on the right) will appear. This is the management console window for the server application.

In the **Menu** bar, there are two options available, **Server** and **Help**. Under the **Server** menu we can **Start**, **Stop** or **Exit** the application. Alternatively, right under the **Server** menu option, there are also start and stop icons that do exactly the same thing. Under the **Help** menu option, there is an **About** option that will, after being clicked, display the name, version and copyright details of this application.



Software Installation Central WifiManager Server Application

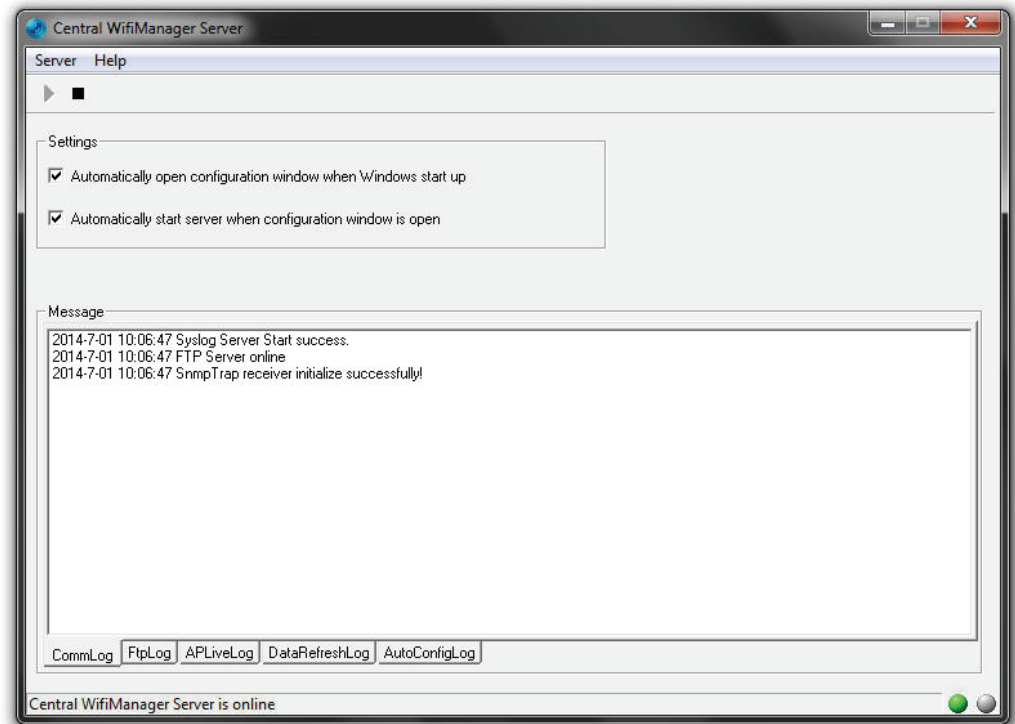
In the **Settings** section, we can select to **Automatically open configuration window when Windows start up** and **Automatically start server when configuration window is open**. Select these options if needed.

After this, there server can be started by click either the start icon or being selecting **Start** in the **Server** menu option.

NOTE: When clicking the close icon, on the far upper right corner, this application will close and exit. The server will not be running in the background. Click the minimize icon to close this window and allow the server application to run in the background.

When the server is up and running, the left circle icon, at the far bottom right corner, will display green. When the server is not running the right circle icon, at the far bottom right corner, will display red.

To view log entries about the System, FTP Connectivity, Live Access Points, Data Transmissions and Automatic Configurations, tabs at the bottom of the **Message** section can be selected.

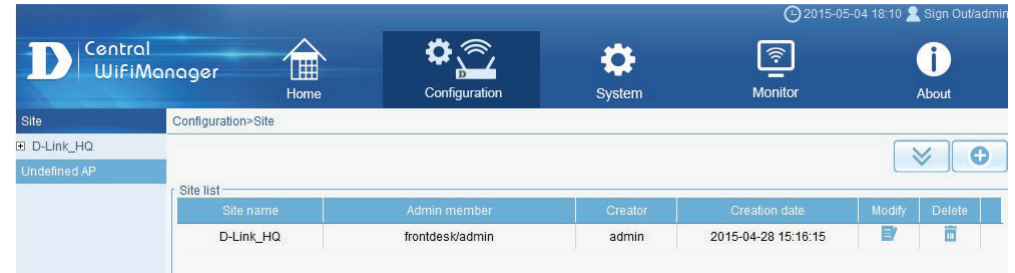


Software Installation Access Point Installation Tool

The Access Point Installation Tool is an additional utility that complements the D-Link Central WifiManager. This utility can be used to scan for new D-Link access points in the network, regardless of what IP range they are configured in, and then pre-configure them to be used in the Central WifiManager. To add new Access Points into the CWM, we need to run Access Point Installation Utility for CWM first. This is required to provide initial synchronization (IP address of the CWM server and authentication information) of APs with the CWM. Once the APs are synchronized with CWM, we can use the CWM: 'Uploading Configuration' option, to push new configuration or any amended configuration remotely to the APs.

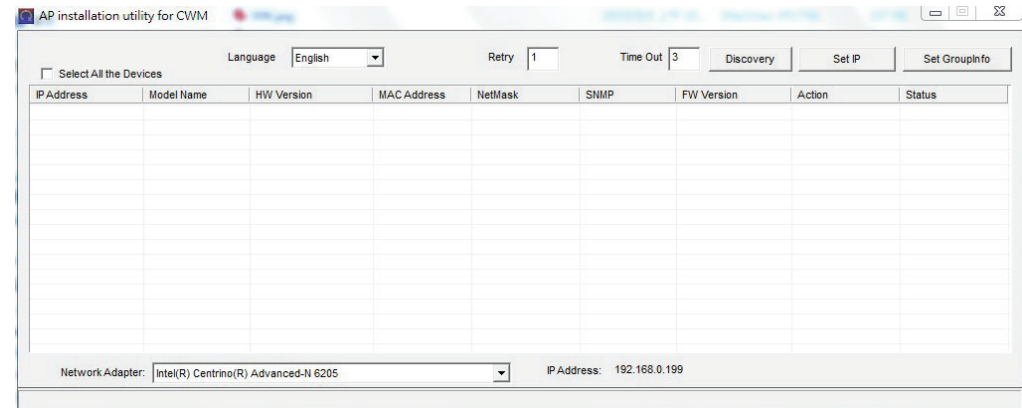
The AP installation tool can download from Configuration>Site

Click the  to download the Access Point Installation Tool



After opening the Access Point Installation Tool, the following window will be available.

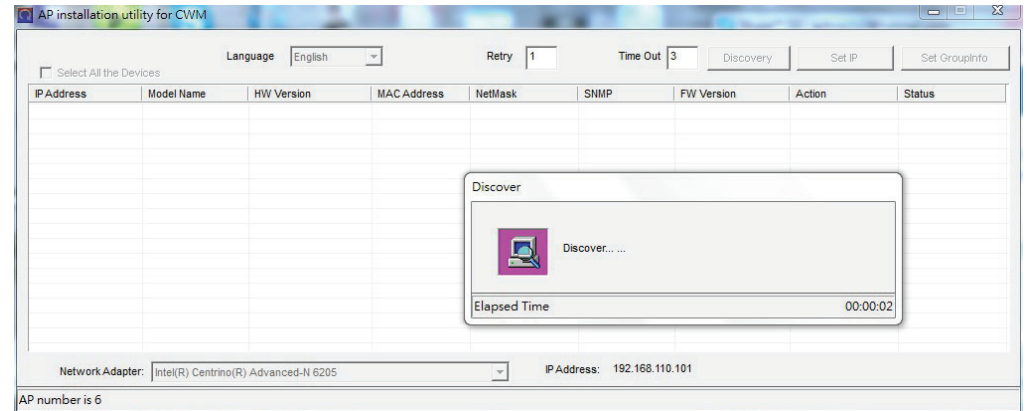
Click the **Discovery** button, to scan for D-Link access points that are connected to the network with an Ethernet cable.



Software Installation

Access Point Installation Tool

After clicking the **Discovery** button, this utility will scan the network for D-Link access points that are connected to the network with an Ethernet cable. This utility will find D-Link access points regardless of what IP address they're configured in.



Software Installation Access Point Installation Tool

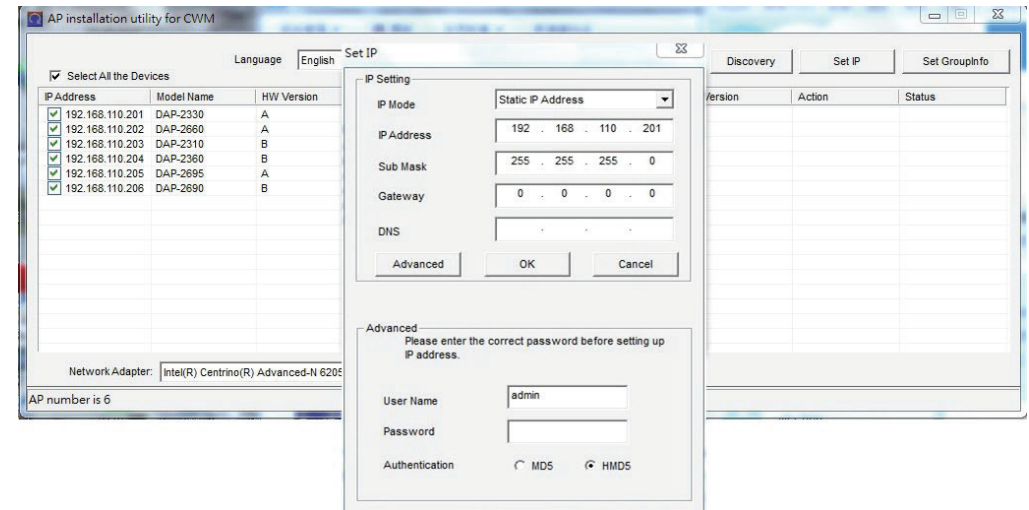
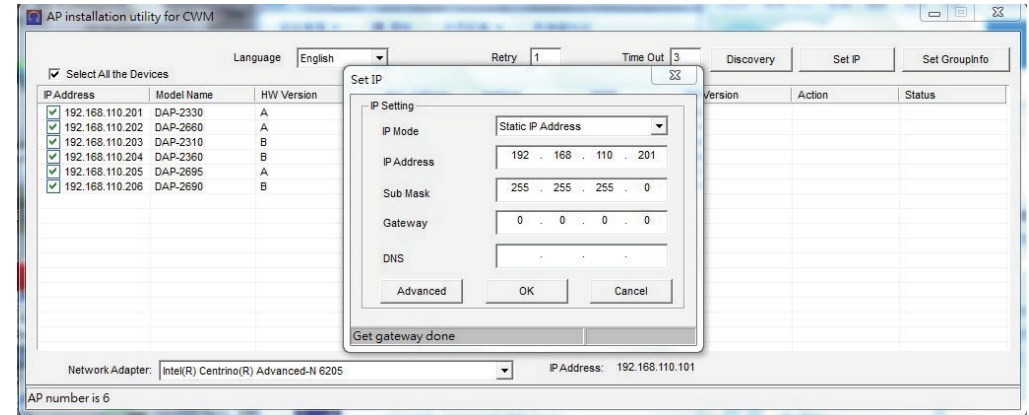
To change the IP address of an access point discovered, select the check box next to it and click the **Set IP** button.

After clicking the Set IP button, the following parameters can be configured:

Parameter	Description
IP Mode	Select the IP mode for the access point here. Options to choose from are Static IP Address , to manually configure the IP settings, and Dynamic IP Address , to allow a DHCP server to automatically assign the IP settings to the access point.
IP Address	Enter the new IP address for the access point here.
Sub Mask	Enter the new subnet mask for the access point here.
Gateway	Enter the gateway's IP address for the access point here.
DNS	Enter the DNS address for the access point here.
User Name	After clicking the Advanced button, we can enter the login username of the access point here.
Password	After clicking the Advanced button, we can enter the login password of the access point here.
Authentication	After clicking the Advanced button, we can select the login authentication encryption method used. Options to choose from are MD5 and HMD5 .

Click the **OK** button to accept the changes made.

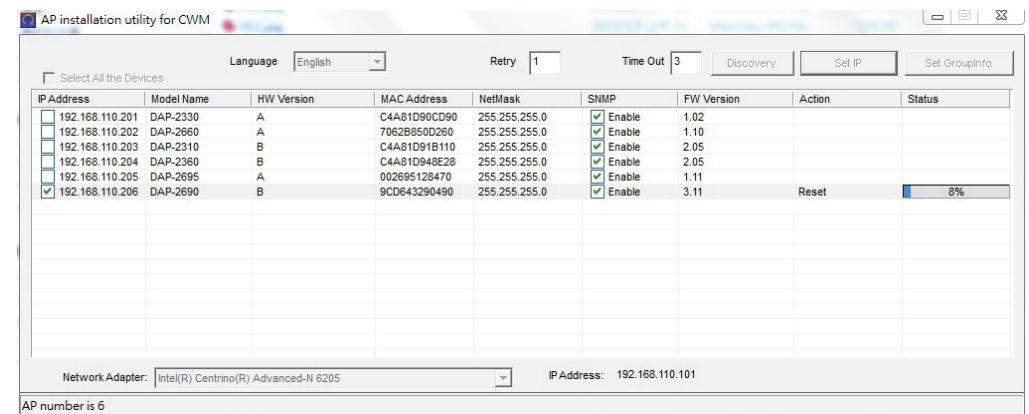
Click the **Cancel** button to discard the changes made.



Software Installation Access Point Installation Tool

After clicking the **OK** button to set the IP address, the access point will be configured and some time will be given for the access point to restart after the new IP address was applied.

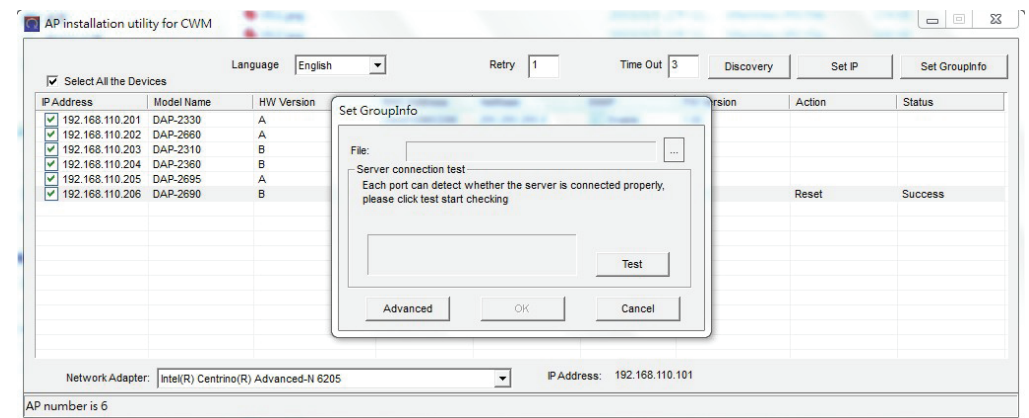
The **Status** parameter will display the progress of the IP address configuration and access point reboot.



This utility also allows us to upload the network data file directly to the access point to configure the group information that this access point will use to identify in which network it belongs.

Click the **Set GroupInfo** button to upload the network data file. After click the **Set GroupInfo** button, we can click on the "..." button to navigate to the saved network data file on the computer and then upload it.

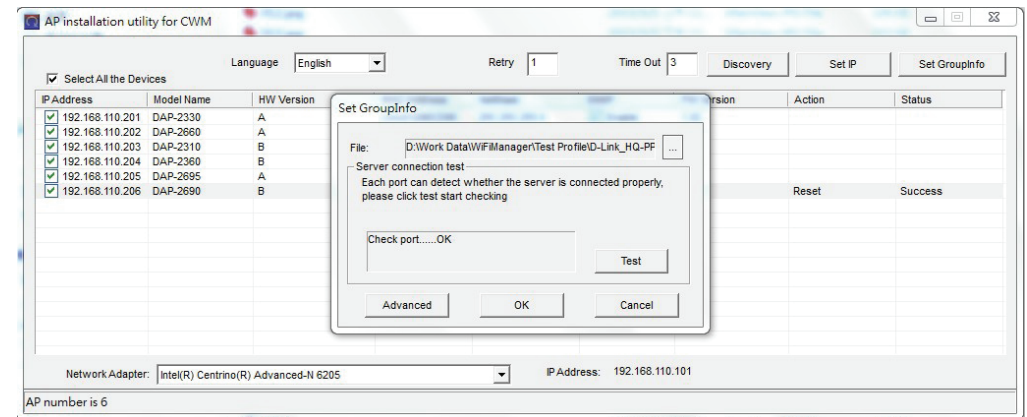
Click the **Test** button to test if the data file is in fact a valid network data file. Click the **Advanced** button to use advanced login options for the access point as discussed earlier.



Software Installation Access Point Installation Tool

After clicking the **Test** button to successfully test if the network data file is valid, the following message will be displayed.

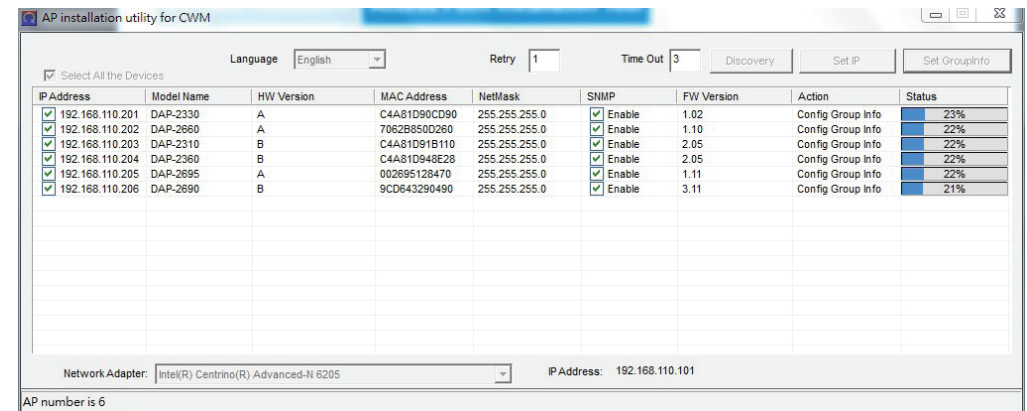
Click the **OK** button to initiate the upload
Click the **Cancel** button to cancel the upload.



After clicking the **OK** button, the network data file will be uploaded, the access point will be configured based on the settings within the data file, and will then reboot.

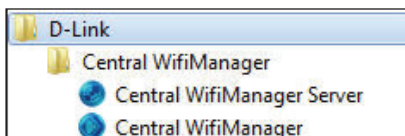
The **Status** parameter will display the progress of the configuration.

For more information about configuring networks and generating network data files used in this upload, refer to “**Network**” on page 26.



Central WifiManager Configuration

In this section, we'll discuss the Central WifiManager client application. After the installation was completed the following applications will be available.



Click the **Central WifiManager** option to open the client application.

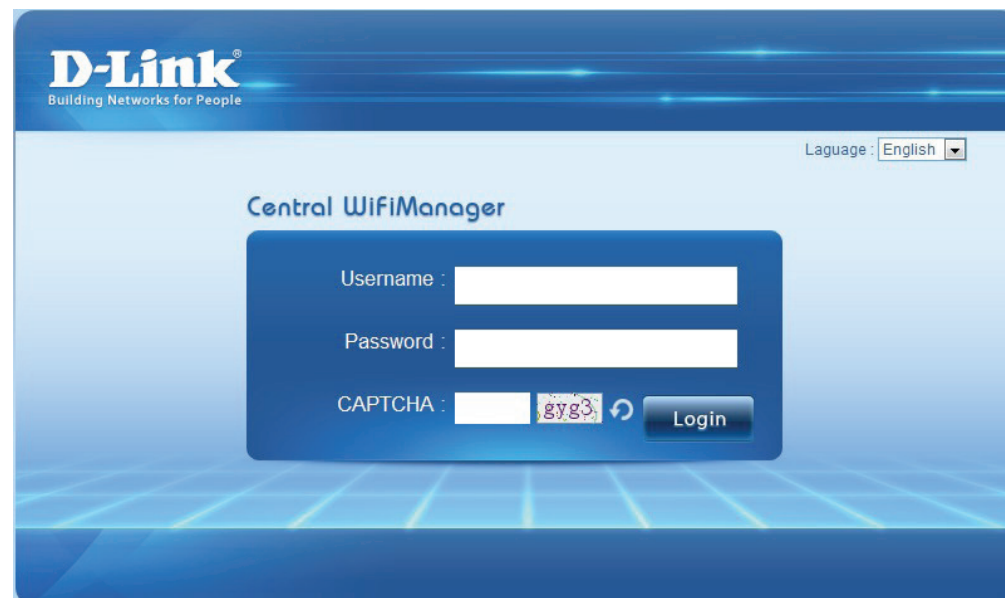
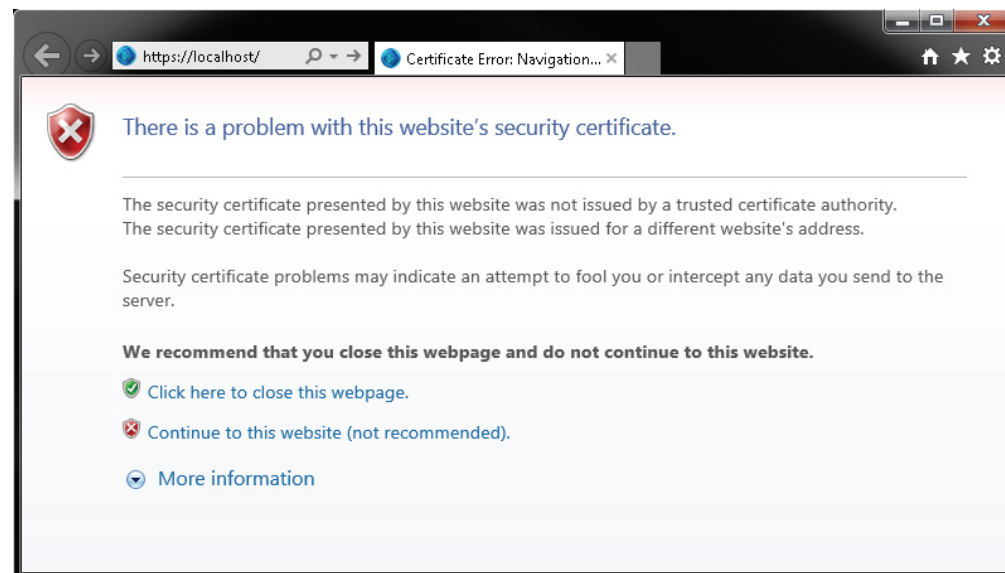
The Central WifiManager uses a secure HTTPS connection to the Central WifiManager Server. By default, this application will open the default Web browser and connect the to **localhost**, which is the local means of connecting to the same PC's own IP address. <\$\$\$Certificate information needed\$\$\$>

Alternatively, from a remote computer, we can connect to the Central WifiManager Server by entering the IP address of the computer that has the server application installed into the web browser, thus it is not needed to install the software on the remote computer. Open the web browser on the remote computer (Internet Explorer or Google Chrome are recommend) and enter for example `https://192.168.10.1` or `https://domain-name.com` (where 192.168.10.1 or domain-name.com is the IP address or domain name of the computer running the CWM server) in the web browser's address bar and press **ENTER** to enter the CWM management interface.

NOTE: Connection to the Central WifiManager Server uses a secure HTTPS connection.

After the Web browser was open and connection to the server was made successfully, a login window will appear. Enter the login user name and password in this spaces provided and click **Login** to enter the Central WifiManager Configuration.

NOTE: By default, the user name and password is **admin**. The default language is English and also support Italian, French, Spanish, German, Korean, Russian, Simplified and Traditional Chinese.



After successfully logging into the server, the **Dashboard** page will be available. On this page, summarized information of the connected access points and wireless clients will be displayed.

After configuring sites, a list of sites will be available for selection in the site drop-down menu.

Underneath the site drop-down menu, the following four blocks with pie charts can be seen.

Block	Description
Station	In this block the number of wireless clients, connected to the access points in this network, will be displayed per wireless frequency supported. The pie chart illustrate this information visually.
Band	In this block the number of wireless frequency bands, hosted by the access points in this network, will be displayed per frequency band supported. The pie chart illustrates this information visually.
Model	In this block the number of access points in this network will be displayed per product code. The pie chart illustrates this information visually.
Access Point	In this block the number of online and offline access points will be displayed per status. The pie chart illustrates this information visually.

In the **Station Detail** table, a list of connected wireless clients will be displayed with the basic information about them.

The screenshot shows the Central WifiManager Dashboard interface. At the top, there is a navigation bar with 'Home', 'Configuration', 'System', 'Monitor', and 'About' options. The main content area is titled 'Home>Dashboard' and includes a 'Site' dropdown menu set to 'All sites'. Below this, there are four pie charts representing different categories: Station, Band, Model, and Access point. Each chart is accompanied by a small table showing the data for each category. At the bottom, there is a 'Station detail' table with columns for No., MAC address, IP address, Alias, Band, Authentication, RSSI, SSID, and Power save mode.

Band	Sum
2.4GHz	0
5GHz	1

Band	Sum
2.4GHz	4
5GHz	3

Model	Sum
DAP-2360	1
DAP-2553	1
DAP-2660	1
DAP-2690	1

Status	Sum
Off line AP	2
On line AP	4

No.	MAC address	IP address	Alias	Band	Authentication	RSSI	SSID	Power save mode
1	A088B4E4C400	192.168.0.103	Click to set alias	N	WPA2-Personal	91	WiFiManager50	OFF

CWM Configuration

Home


Site


Device View

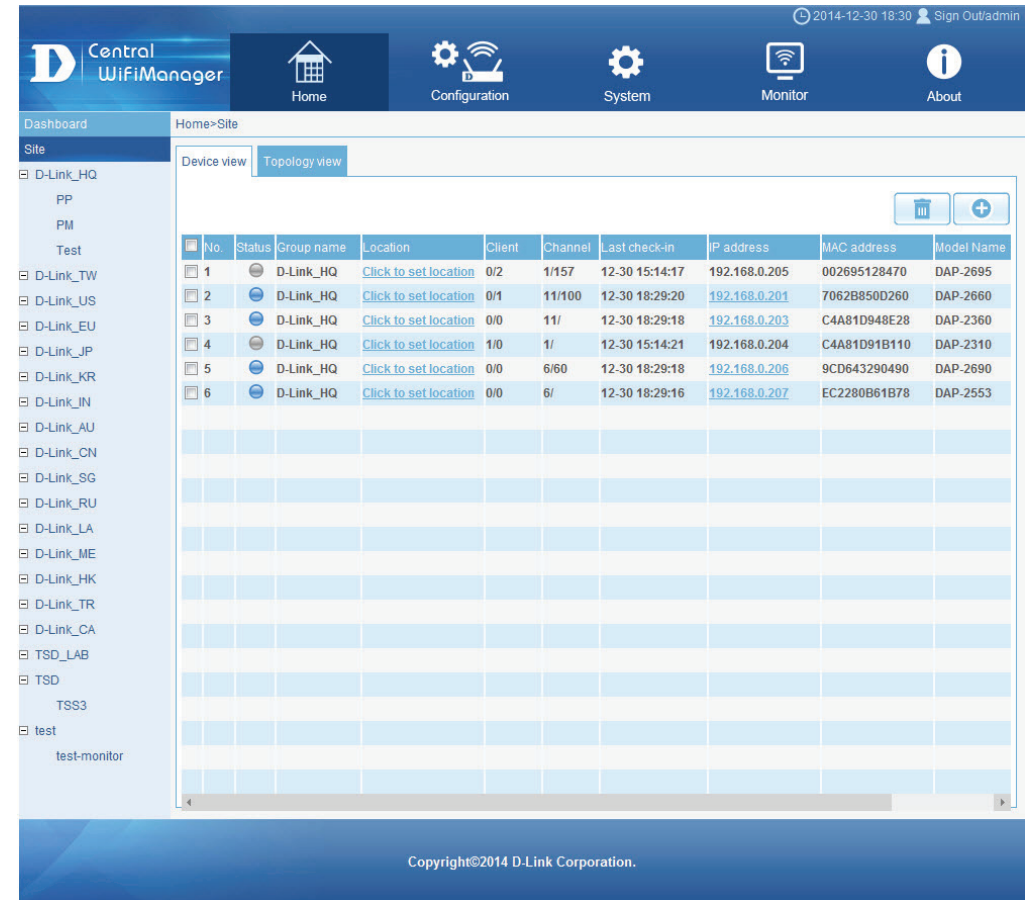
On this page, a list of configured sites will be displayed. For more information on how to create or configure sites, refer to “**Create Site**” on page 24. For this example, we created a site called **Headquarters** and within the site we created a network called **Server-Room**.

For more information on how to create or configure networks, refer to “**Create Network**” on page 27.

In the **Device View** tab, a list of access points will be displayed that was associated with the **Headquarters** site. More information about the access points will be displayed in the table columns. To view more detailed information about a specific access point, click on the IP address of that access point.

Click the  icon to remove an access point from this network.

Click the  icon to select what information will be displayed of your site or network.



No.	Status	Group name	Location	Client	Channel	Last check-in	IP address	MAC address	Model Name
1	Online	D-Link_HQ	Click to set location	0/2	1/157	12-30 15:14:17	192.168.0.205	002695128470	DAP-2695
2	Online	D-Link_HQ	Click to set location	0/1	11/100	12-30 18:29:20	192.168.0.201	7062B850D260	DAP-2660
3	Online	D-Link_HQ	Click to set location	0/0	11/	12-30 18:29:18	192.168.0.203	C4A81D948E28	DAP-2360
4	Online	D-Link_HQ	Click to set location	1/0	1/	12-30 15:14:21	192.168.0.204	C4A81D91B110	DAP-2310
5	Online	D-Link_HQ	Click to set location	0/0	6/60	12-30 18:29:18	192.168.0.206	9CD643290490	DAP-2690
6	Online	D-Link_HQ	Click to set location	0/0	6/	12-30 18:29:16	192.168.0.207	EC2280B61B78	DAP-2553

Copyright©2014 D-Link Corporation.

CWM Configuration Home Site **Topology View**

On this page, all the devices connected to the specified site will be displayed visually. The following items can be found on this page.

Item	Description
Add Topology	On the top, right of the viewing area, there is a + icon. Click this icon to add a custom topology.
Edit Topology	On the top, right of the viewing area, there is an i icon. Click this icon to modify the newly added topology's name.
Delete Topology	On the right of the topology tabs, there is an x icon. Click this icon to remove the custom topologies created. The all topology, which is automatically generated, cannot be deleted.
Map Size	The map size of the topology view can be modified. Enter the width and height of this view in the text boxes and click Submit to accept the changes made. These values must be between 800 and 8000.
Cursor	Select this option to select an item individually.
Guide	Select this option to make the guides visible in the topology.
Add Device	Select this option to add access points, that have been associated with this site, into the topology.
Add Background	Select this option to add a custom background image to the topology. Image formats supported are JPG, JPEG, GIF and PNG.
Pen	Select this option to manually draw a connection line from one device to another. After drawing the connection line, it can be specified as either wired or wireless and the color and line thickness can be customized.

The screenshot displays the Central WifiManager software interface in the Topology View. The main area shows a network diagram with three DAP-2660 access points connected to a central station. The interface includes a navigation menu on the left, a toolbar with various drawing tools, and a top navigation bar with options like Home, Configuration, System, Monitor, and About. The map size is set to 1000 width and 1000 height.

Copyright ©2014 D-Link Corporation.

[CWM Configuration](#)[Home](#)[Site](#)[Topology View](#)

Parameter	Description
Drag	Select this option to enable the function to simply select and move the objects and the background of the topology into place.
Save	Select this option to save the topology.
PC (Null)	This icons illustrates the management PC, where the Central WifiManager Server application is installed.
Access Points	These icons illustrate the access points located at the site and there connection relation with each other. Double click on any access point icon to view more detailed information about the selected access point.

CWM Configuration

Configuration

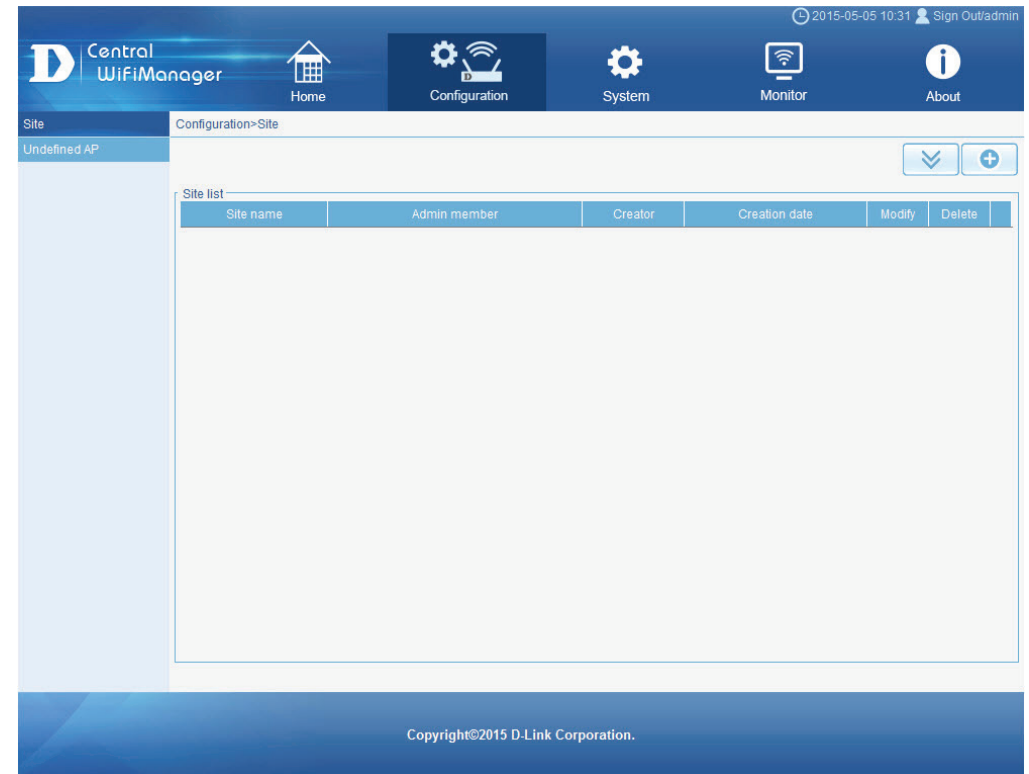
Site

On this page we can view, create and configure logical sites and networks that are related to the physical locations of the wireless devices in the network. Wireless devices at these sites can unanimously and effortlessly be managed and maintained through the use of this application.

Sites and networks that have already been configured will be displayed under the **Site** option on the left panel. Also, after clicking on the **Site** option in the left panel, the list of configured sites will be displayed in the **Site List** table on the main page.

Click the  button to add a new site.

Click the  to download the Access Point Installation Tool



The screenshot displays the Central WifiManager Configuration interface. The top navigation bar includes the D-Link logo, the text "Central WifiManager", and icons for Home, Configuration, System, Monitor, and About. The main content area is titled "Configuration > Site" and features a left sidebar with "Site" and "Undefined AP" options. The main area contains a "Site list" table with the following columns: Site name, Admin member, Creator, Creation date, Modify, and Delete. The table is currently empty. A footer at the bottom of the page reads "Copyright©2015 D-Link Corporation."

CWM Configuration

Configuration

Site

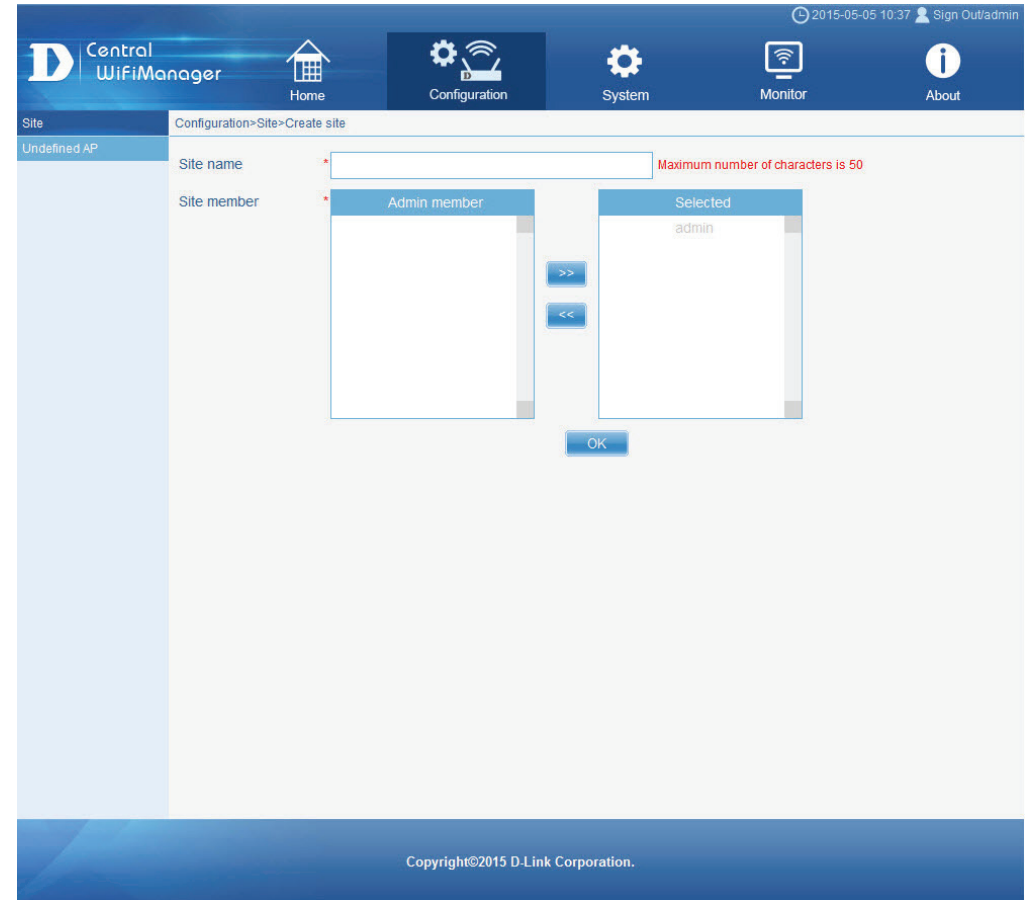
Create Site

After clicking the  button to add a new site, the following page will be available. On this page, users can create sites and also assign member accounts to each site.

The following parameters can be configured:

Parameter	Description
Site name	Enter the new site's name here. This name can be up to 50 characters long.
Site member	Select the member accounts that will be added to this site in the left box and click >> to add them to the Selected list in the right box. To remove a member account from the selected list, select it and click << to remove the account.

Click the **OK** button to create the new site.




The screenshot displays the 'Create site' configuration page in the Central WifiManager interface. The page title is 'Configuration>Site>Create site'. The 'Site name' field is empty and has a red asterisk next to it, with a red error message 'Maximum number of characters is 50' to its right. Below the 'Site name' field are two lists: 'Admin member' (empty) and 'Selected' (containing 'admin'). Between the lists are '>>' and '<<' buttons. An 'OK' button is located below the 'Selected' list. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'.


CWM Configuration


Configuration

Site

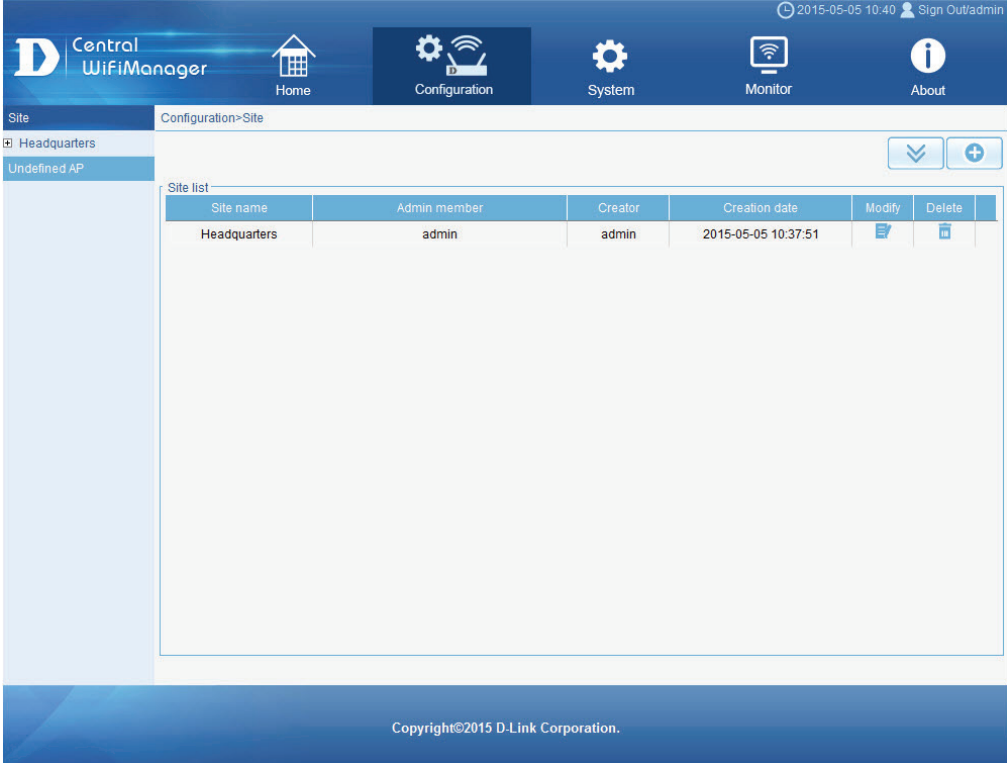
After creating a new site, it will be displayed in the **Site List** table. In this example, we created a site called **Headquarters**.

Click the  button to add another site.



Click the  icon to modify an existing site.

Click the  icon to delete an existing site.

Click the  to download the Access Point Installation Tool



The screenshot displays the Central WifiManager Configuration interface. The top navigation bar includes the D-Link logo, the text 'Central WifiManager', and several menu items: Home, Configuration, System, Monitor, and About. The 'Configuration' menu is currently selected. Below the navigation bar, the page title is 'Configuration > Site'. On the left side, there is a sidebar with a tree view showing 'Site' (expanded) and 'Undefined AP'. The main content area features a 'Site list' table with the following data:

Site name	Admin member	Creator	Creation date	Modify	Delete
Headquarters	admin	admin	2015-05-05 10:37:51		

At the bottom of the page, the copyright notice reads: Copyright©2015 D-Link Corporation.


CWM Configuration

Configuration

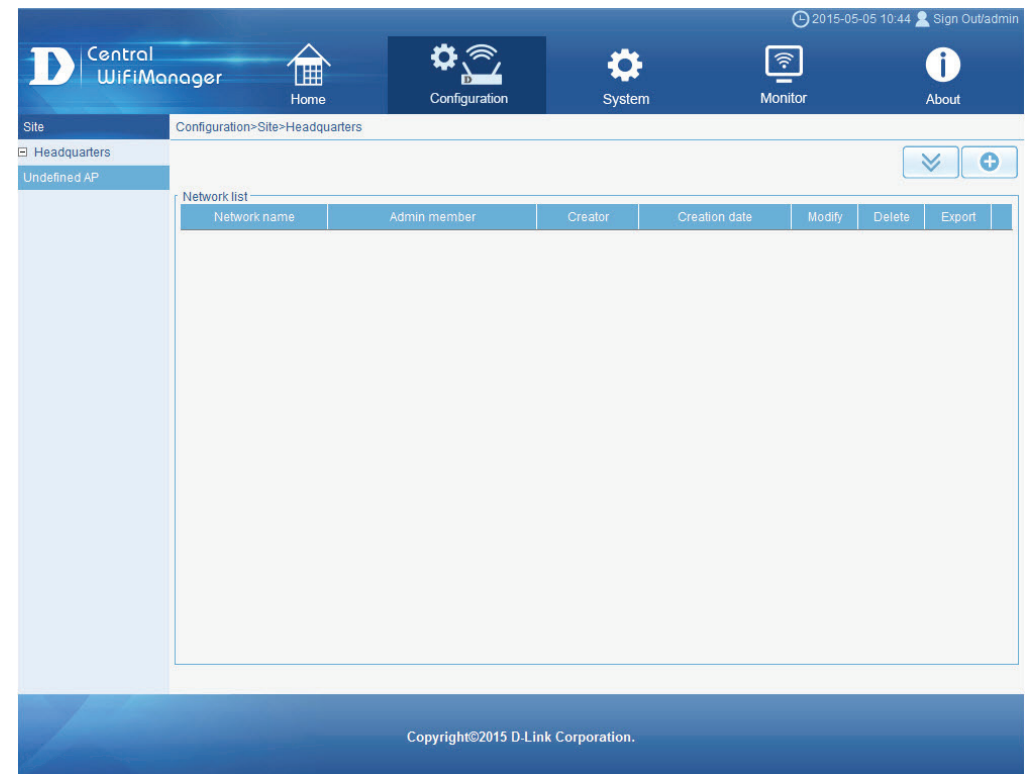
Site

Network


After clicking on the site link called **Headquarters**, in the left panel, we can see the list of networks that have been created for the site in the **Network List** table on the main page.

Click the  button to add a new network for this site.

Click the  to download the Access Point Installation Tool



The screenshot displays the D-Link Central WifiManager Configuration interface. The top navigation bar includes the D-Link logo, the text "Central WifiManager", and several icons: Home, Configuration, System, Monitor, and About. The current page is "Configuration > Site > Headquarters". The left sidebar shows a tree view with "Headquarters" selected and "Undefined AP" below it. The main content area is titled "Network list" and contains a table with the following columns: Network name, Admin member, Creator, Creation date, Modify, Delete, and Export. The table is currently empty. At the bottom of the page, there is a copyright notice: "Copyright©2015 D-Link Corporation."

After clicking the  button to add a new network, the following page will be available. On this page, users can create networks and also assign member accounts to each network.

The following parameters can be configured:

Parameter	Description
Network name	Enter the new network's name here. This name can be up to 50 characters long.
Network member	Select the member accounts that will be added to this network in the left box and click >> to add them to the Selected list in the right box. To remove a member account from the selected list, select it and click << to remove the account.

Click the **OK** button to create the new network.

CWM Configuration

Configuration

Site

Network

After creating a new network, it will be displayed in the **Network List** table. In this example, we created a network called **Server-Room**.

Click the  to download the Access Point Installation Tool

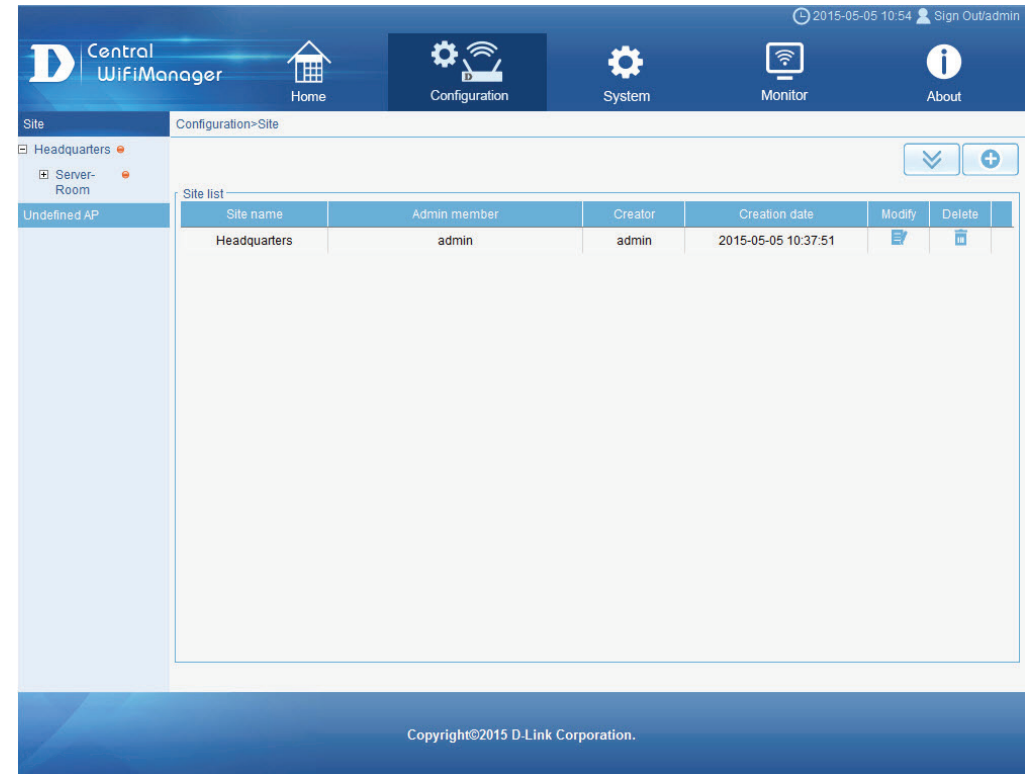
Click the  button to add another network.

Click the  icon to modify an existing network.



Click the  icon to delete an existing network.

Click the  icon to download the **data file** of this network, that can be **uploaded** to an **access point** to quickly configure an access point to identify with this network.

For more information about how to upload the network data file to an access point for seamless network association, refer to “**Access Point Installation Tool**” on page 13.



The screenshot shows the Central WifiManager Configuration interface. The top navigation bar includes Home, Configuration, System, Monitor, and About. The left sidebar shows a tree view with 'Headquarters' and 'Server-Room' under 'Site'. The main content area displays a 'Site list' table with the following data:

Site name	Admin member	Creator	Creation date	Modify	Delete
Headquarters	admin	admin	2015-05-05 10:37:51		

The interface also includes a copyright notice at the bottom: Copyright©2015 D-Link Corporation.

CWM Configuration


Configuration

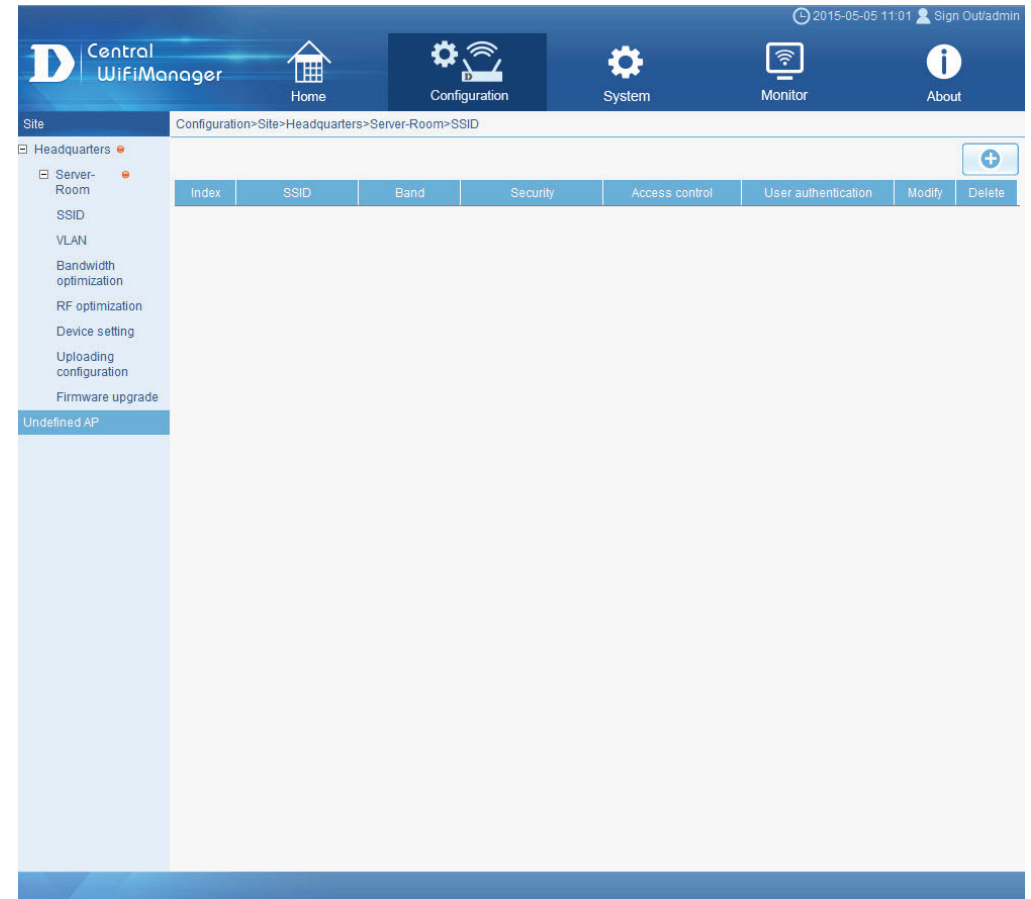
Site

Network

SSID

After clicking on the network link called **Server-Room**, in the left panel, a feature rich configuration page is available where users can manually configure settings that will be applied to all access points available in the network selected. On this page we can now create a wireless network profile called **SSID**.

Click the  button to add a new SSID.



The screenshot displays the D-Link Central WifiManager configuration interface. The top navigation bar includes the D-Link logo, the text "Central WifiManager", and icons for Home, Configuration, System, Monitor, and About. The current page is titled "Configuration>Site>Headquarters>Server-Room>SSID". The left sidebar shows a tree view with "Headquarters" expanded, and "Server-Room" selected. Under "Server-Room", the following options are listed: SSID, VLAN, Bandwidth optimization, RF optimization, Device setting, Uploading configuration, and Firmware upgrade. The "Undefined AP" section is currently selected. The main content area shows a table with the following columns: Index, SSID, Band, Security, Access control, User authentication, Modify, and Delete. A plus icon (+) is visible in the top right corner of the table area.

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

After adding a new SSID, the following page will be available. In the **Basic Settings** section, we can configure the following:

Parameter	Description
Band	Select the wireless frequency band that will be used for this network here. Options to choose from are 2.4G and 5G .
Index	Select the SSID index that will be used fore this network here. Options to choose from are Primary and SSID1 to SSID7 .
SSID	Enter the wireless network name for this network here. This is name is also called the SSID of the wireless network.
SSID Broadcast	Select to Enable or Disable the wireless SSID visibility here.
WMM (Wi-Fi Multimedia)	Select to Enable or Disable the Wi-Fi multimedia features here.
Security	Select the wireless security that will be used by this wireless network here. Options to choose from are Open System , Shared Key , WPA-Personal , WPA-Enterprise , WPA2-Personal , WPA2-Enterprise , WPA-Auto-Personal , and WPA-Auto-Enterprise .

In the following sections we'll discuss the wireless security options that are available to networks managed by this application.

The screenshot shows the Central WifiManager configuration interface. The top navigation bar includes the D-Link logo, 'Central WifiManager', and icons for Home, Configuration, System, Monitor, and About. The user is logged in as 'admin' on 2015-05-05 at 11:05. The breadcrumb trail is 'Configuration > Site > Headquarters > Server-Room > SSID'. The left sidebar shows a tree view with 'Headquarters' expanded to 'Server-Room', which contains 'SSID', 'VLAN', 'Bandwidth optimization', 'RF optimization', 'Device setting', 'Uploading configuration', and 'Firmware upgrade'. The main content area is titled 'Basic settings' and is divided into three sections:

- Wireless settings:** Band (2.4G), Index (Primary), SSID (text input), SSID broadcast (Enable), WMM (Wi-Fi Multimedia) (Enable), and Security (Open System).
- WPA settings:** Encryption (Disable), Key size (64 Bits), Key type (HEX), Key index (1), and Key value (text input).
- Access control:** MAC address (text input), Add button, Action (Disable), and a table with columns 'No.', 'MAC address', and 'Delete'.

At the bottom, there is a 'User authentication' section with 'Authentication type' set to 'Disable'. 'Save' and 'Back' buttons are located at the bottom right of the configuration area. The footer contains the text 'Copyright©2015 D-Link Corporation.'

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

After selecting the WEP **Open System** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Encryption	Select this option to Enable or Disable the WEP Open System encryption method for this network.
Key Size	Select the WEP key size here. Options to choose from are 64 Bits , 128 Bits , and 256 Bits .
Key Type	Select the WEP key type here. Options to choose from are HEX and ASCII .
Key Index	Select which key in the index of four will be used for this network. Options to choose from are First , Second , Third , and Fourth .
Key Value	Enter the open system WEP encryption key here, based on the selections made.

The screenshot shows the 'Basic Settings' configuration page. Under 'Wireless Settings', the 'Band' is set to 2.4G, 'Index' to Primary, and 'Security' to Open System. Under 'Key Settings', 'Encryption' is set to Disable, 'Key Size' to 64 Bits, 'Key Type' to HEX, and 'Key Index' to First. The 'Key Value' field is empty.

After selecting the WEP **Shared Key** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Encryption	Select this option to Enable or Disable the WEP Shared Key encryption method for this network.
Key Size	Select the WEP key size here. Options to choose from are 64 Bits , 128 Bits , and 256 Bits .
Key Type	Select the WEP key type here. Options to choose from are HEX and ASCII .
Key Index	Select which key in the index of four will be used for this network. Options to choose from are First , Second , Third , and Fourth .
Key Value	Enter the open system WEP encryption key here, based on the selections made.

The screenshot shows the 'Basic Settings' configuration page. Under 'Wireless Settings', the 'Band' is set to 2.4G, 'Index' to Primary, and 'Security' to Shared Key. Under 'Key Settings', 'Encryption' is set to Enable, 'Key Size' to 64 Bits, 'Key Type' to HEX, and 'Key Index' to First. The 'Key Value' field is empty.

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

After selecting the **WPA-Personal** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA cipher type here. Options to choose from are Auto, AES, and TKIP .
Group Key Update Interval	Enter the WPA group key update interval value here. By default, this value is 3600.
Pass Phrase	Enter the secret pass phrase used here.

After selecting the **WPA-Enterprise** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA cipher type here. Options to choose from are Auto, AES, and TKIP .
Group Key Update Interval	Enter the WPA group key update interval value here. By default, this value is 3600.
RADIUS Server	Enter the RADIUS server's IP address here.
Port	Enter the RADIUS server's port number used here. By default, this port number is 1812.
RADIUS Secret	Enter the RADIUS secret pass phrase used here.

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

After selecting the **WPA2-Personal** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA2 cipher type here. Options to choose from are Auto , AES , and TKIP .
Group Key Update Interval	Enter the WPA2 group key update interval value here. By default, this value is 3600.
Pass Phrase	Enter the secret pass phrase used here.

After selecting the **WPA2-Enterprise** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA2 cipher type here. Options to choose from are Auto , AES , and TKIP .
Group Key Update Interval	Enter the WPA2 group key update interval value here. By default, this value is 3600.
RADIUS Server	Enter the RADIUS server's IP address here.
Port	Enter the RADIUS server's port number used here. By default, this port number is 1812.
RADIUS Secret	Enter the RADIUS secret pass phrase used here.

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

After selecting the **WPA-Auto-Personal** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA/WPA2 cipher type here. Options to choose from are Auto , AES , and TKIP .
Group Key Update Interval	Enter the WPA/WPA2 group key update interval value here. By default, this value is 3600.
Pass Phrase	Enter the secret pass phrase used here.

Basic settings

Wireless settings

Band: 2.4G

Index: SSID1

SSID: []

SSID broadcast: Enable

WMM (Wi-Fi Multimedia): Enable

Security: WPA-Auto-Personal

WPA settings

Encryption type: Auto

Group key update interval: 3600

Passphrase: []

RADIUS server: [] Port: 1812

RADIUS secret: []

After selecting the **WPA-Auto-Enterprise** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA/WPA2 cipher type here. Options to choose from are Auto , AES , and TKIP .
Group Key Update Interval	Enter the WPA/WPA2 group key update interval value here. By default, this value is 3600.
RADIUS Server	Enter the RADIUS server's IP address here.
Port	Enter the RADIUS server's port number used here. By default, this port number is 1812.
RADIUS Secret	Enter the RADIUS secret pass phrase used here.

Basic settings

Wireless settings

Band: 2.4G

Index: SSID1

SSID: []

SSID broadcast: Enable

WMM (Wi-Fi Multimedia): Enable

Security: WPA-Auto-Enterprise

WPA settings

Encryption type: Auto

Group key update interval: 3600

Passphrase: []

RADIUS server: [] Port: 1812

RADIUS secret: []

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

In the **Access Control** section we can configure which network devices can have access to the network or not by specifying the MAC of the accepted or rejected devices. The following parameters can be configured.

Parameter	Description
MAC Address	Enter the MAC address of the networking device that will be used for this configuration here.
Action	Select the action that will be applied to the networking device. Option to choose from are Disable , Accept and Reject .

A list of configured entries will be displayed in the table.

Click the  icon to remove a specific entry.

In the **User Authentication** section we can configure the authentication method that will be applied to all the wireless clients that connect to access point in this network. The following parameters can be configured.

Parameter	Description
Authentication Type	Select the authentication type that will be applied to the wireless clients in this network. Options to choose from are Disable , Web Redirection Only , Username/password , Remote RADIUS , LDAP , POP3 and Passcode . After selecting Disable as the authentication type, this feature will be disabled.

Access control

MAC address: Action:

No.	MAC address	Delete

User authentication

Authentication type:

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

After selecting **Web Redirection Only** as the **Authentication Type**, we can configure the redirection website URL that will be applied to each wireless client in this network.

The following parameters can be configured.

Parameter	Description
Web redirection	Select this option to enable the website redirection feature.
Website	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https:// , enter the URL of the website that will be used in the space provided.

Click the **Save** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the main page.

After selecting **Username/password** as the **Authentication Type**, we can apply local authentication to each wireless client in this network. Local authentication means that no external server is needed to help with the authentication process. Authentication is applied based on restricted subnets, username and password authentication based on the accounts created here and the group that they belong to.

The following parameters can be configured.

Parameter	Description
Session timeout	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.
IP Address	Enter the IP address or network address that will be used in the IP filter rule here. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.
Subnet Mask	Enter the subnet mask of the IP address or networks address that will be filtered here. For example, 255.255.255.0.

IP address	Subnet mask	Delete
192.168.70.66	255.255.255.0	

Click the **Add** button to add the new IP filter rule.

Click the icon to delete an existing rule.

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

Parameter	Description
Username	Enter the username that the wireless clients should use here.
Password	Enter the password that the wireless clients should use here.

Click the **Add** button to add a new user account.

Click the **Clear** button to clear out the information entered in the fields.



Click the  icon to modify an existing account.

Click the  icon to delete an existing user account.

User/password settings

Username

Password

Username	Modify	Delete
user1		

Parameter	Description
Web redirection	Select this option to enable the website redirection feature.
Website	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https:// , enter the URL of the website that will be used in the space provided.
Choose template	Select the login page that will be used here.

After selecting the style to use, click the **Preview** button to preview the selected style.

Click the **Upload login file** button to upload a new style.

Click the [Delete the style](#) link to delete the selected style.

Click the [Download Template](#) link to download the style template.

Web redirection

Website :

Splash page customization

Choose template: [Delete the template](#) [Download template](#)

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

In the following section we can configure what network devices are allowed to connect to this network by specifying the MAC address of those network devices.

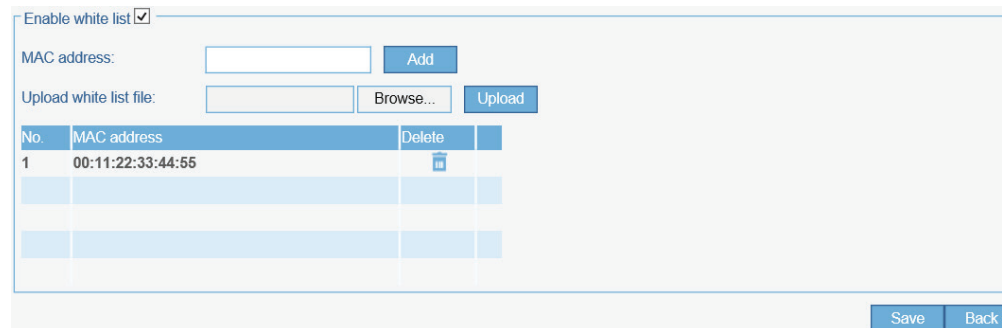
The following parameters can be configured.

Parameter	Description
Enable White List	Select this option to enable the white list feature.
MAC Address	Enter the MAC address of the networking device that will be allowed to connect to this network here. Click Add to then add this MAC address to the white list table.
Upload White List File	To upload a white list file, click Browse and navigate to the white list file, saved on the computer, and then click Upload .

Click the  icon to delete an existing entry.

Click the **Save** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the main page.



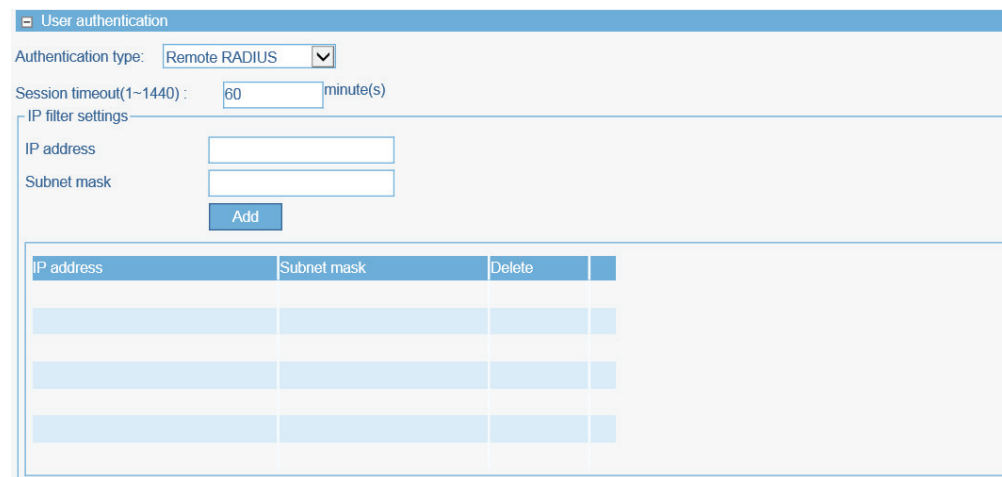
After selecting **Remote RADIUS** as the **Authentication Type**, we can configure access points in this network to act as authenticator devices that will communicate and relay authentication messages to an additional RADIUS server installed in the network.

The following parameters can be configured.

Parameter	Description
Session timeout	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.
IP Address	Enter the IP address or network address that will be used in the IP filter rule here. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.
Subnet Mask	Enter the subnet mask of the IP address or networks address that will be filtered here. For example, 255.255.255.0.

Click the **Add** button to add the new IP filter rule.

Click the  icon to delete an existing rule.



CWM Configuration

Configuration

Site

Network

SSID

Create SSID

Parameter	Description
RADIUS Server	Enter the primary, secondary or third RADIUS server's IP address here.
RADIUS Port	Enter the primary, secondary or third RADIUS server's port number used here. By default this value is 1812.
RADIUS Secret	Enter the primary, secondary or third RADIUS server secret here.
Remote RADIUS type	Select the primary, secondary or third remote RADIUS server type here. Options to choose from are SPAP and MS-CHAPv2 .

Parameter	Description
Web redirection	Select this option to enable the website redirection feature.
Website	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https:// , enter the URL of the website that will be used in the space provided.
Choose template	Select the login page that will be used here.

After selecting the style to use, click the **Preview** button to preview the selected style.
 Click the **Upload login file** button to upload a new style.
 Click the [Delete the style](#) link to delete the selected style.
 Click the [Download Template](#) link to download the style template.

Remote RADIUS settings

RADIUS server settings

RADIUS server: RADIUS port: (1-65535)

RADIUS secret:

Remote RADIUS type:

Secondary RADIUS Server Settings

RADIUS server: RADIUS port: (1-65535)

RADIUS secret:

Remote RADIUS type:

Third RADIUS Server Settings

RADIUS server: RADIUS port: (1-65535)

RADIUS secret:

Remote RADIUS type:

Web redirection

Website:

Splash page customization

Choose template: [Preview](#) [Upload login file](#) [Delete the template](#) [Download template](#)

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

In the following section we can configure what network devices are allowed to connect to this network by specifying the MAC address of those network devices.

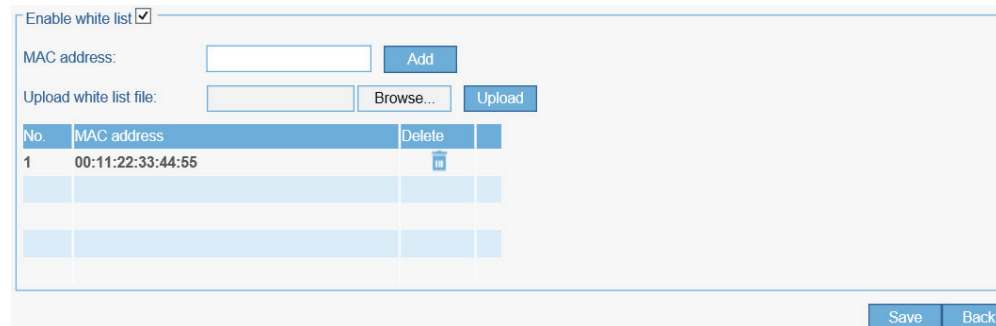
The following parameters can be configured.

Parameter	Description
Enable White List	Select this option to enable the white list feature.
MAC Address	Enter the MAC address of the networking device that will be allowed to connect to this network here. Click Add to then add this MAC address to the white list table.
Upload White List File	To upload a white list file, click Browse and navigate to the white list file, saved on the computer, and then click Upload .

Click the  icon to delete an existing entry.

Click the **Save** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the main page.



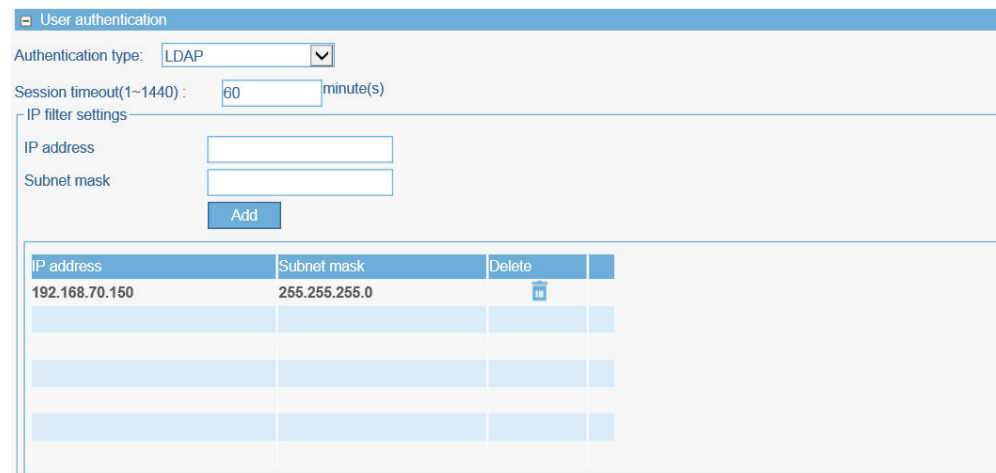
After selecting **LDAP** as the **Authentication Type**, we can configure access points to use an additional LDAP server to handle user authentication in this network.

The following parameters can be configured.

Parameter	Description
Session timeout	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.
IP Address	Enter the IP address or network address that will be used in the IP filter rule here. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.
Subnet Mask	Enter the subnet mask of the IP address or networks address that will be filtered here. For example, 255.255.255.0.

Click the **Add** button to add the new IP filter rule.

Click the  icon to delete an existing rule.



CWM Configuration

Configuration

Site

Network

SSID

Create SSID

Parameter	Description
Server	Enter the LDAP server's IP address here.
Port	Enter the LDAP server's port number used here.
Authenticate Mode	Select the authentication mode that will be used here. Options to choose from are Simple and TLS .
Username	Enter the administrator's username here that will be able to access and search the LDAP database.
Password	Enter the administrator's password here that will be able to access and search the LDAP database.

LDAP settings

Server:

Port:

Authentication mode:

Username:

Password:

Base DN: (ou=,dc=)

Account attribute: (ex.cn)

Identity: Auto copy

Base DN	Enter the base domain name of the LDAP database here. For example, cn=users, dc=test, dc=com means that the wireless client is a member of the group users in the domain test.com .
Account Attribute	Enter the attribute for the account here. For example, cn is used for Windows Server.
Identity	Enter the name of the administrator here. For example, cn=Administrator, cn=users, dc=test, dc=com means for Windows Server, if the administrator is a member of wireless client, it is also a member of the group users in the domain test.com . Alternatively select the Auto Copy option to automatically generate and insert the name of the administrator here based on the Base DN and Account Attribute strings entered.

Parameter	Description
Web redirection	Select this option to enable the website redirection feature.
Website	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https:// , enter the URL of the website that will be used in the space provided.
Choose template	Select the login page that will be used here.

Web redirection

Website:

Splash page customization

Choose template: [Preview](#) [Upload login file](#) [Delete the template](#) [Download template](#)

After selecting the style to use, click the **Preview** button to preview the selected style.
 Click the **Upload login file** button to upload a new style.
 Click the [Delete the style](#) link to delete the selected style.
 Click the [Download Template](#) link to download the style template.

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

In the following section we can configure what network devices are allowed to connect to this network by specifying the MAC address of those network devices.

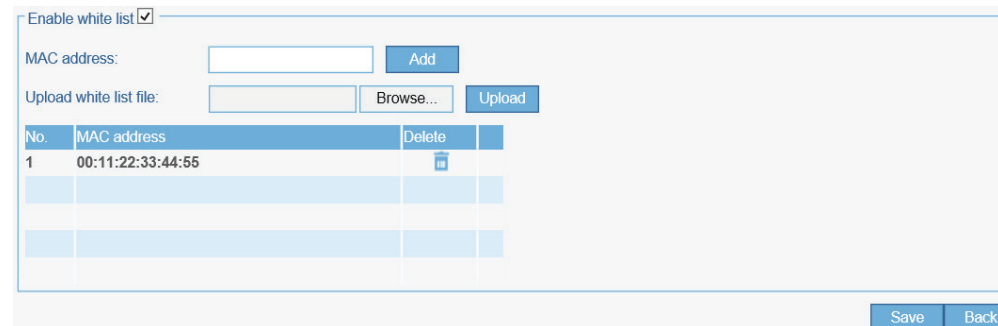
The following parameters can be configured.

Parameter	Description
Enable White List	Select this option to enable the white list feature.
MAC Address	Enter the MAC address of the networking device that will be allowed to connect to this network here. Click Add to then add this MAC address to the white list table.
Upload White List File	To upload a white list file, click Browse and navigate to the white list file, saved on the computer, and then click Upload .

Click the  icon to delete an existing entry.

Click the **Save** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the main page.



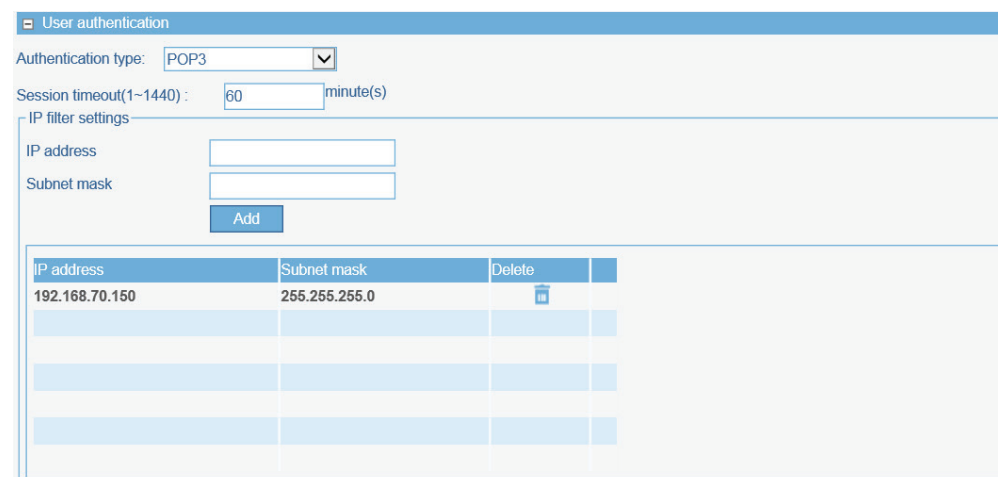
After selecting **POP3** as the **Authentication Type**, we can configure access points to use an additional POP3 server to handle user authentication in this network.

The following parameters can be configured.

Parameter	Description
Session timeout	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.
IP Address	Enter the IP address or network address that will be used in the IP filter rule here. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.
Subnet Mask	Enter the subnet mask of the IP address or networks address that will be filtered here. For example, 255.255.255.0.

Click the **Add** button to add the new IP filter rule.

Click the  icon to delete an existing rule.



CWM Configuration

Configuration

Site

Network

SSID

Create SSID

Parameter	Description
Server	Enter the POP3 server's IP address here.
Port	Enter the POP3 server's port number used here. By default this port number is 110. For the SSL/TLS connection type this value is 995 by default.
Connection Type	Select the POP3 connection type here. Options to choose from are None and SSL/TLS .

POP3 settings

Server:

Port: (1~65535)

Connection type:

Parameter	Description
Web redirection	Select this option to enable the website redirection feature.
Website	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https:// , enter the URL of the website that will be used in the space provided.
Choose template	Select the login page that will be used here.

Web redirection

Website:

Splash page customization


Choose template: [Preview](#) [Upload login file](#) [Delete the template](#) [Download template](#)

After selecting the style to use, click the **Preview** button to preview the selected style.
 Click the **Upload login file** button to upload a new style.
 Click the [Delete the style](#) link to delete the selected style.
 Click the [Download Template](#) link to download the style template.

In the following section we can configure what network devices are allowed to connect to this network by specifying the MAC address of those network devices.

The following parameters can be configured.


Parameter	Description
Enable White List	Select this option to enable the white list feature.
MAC Address	Enter the MAC address of the networking device that will be allowed to connect to this network here. Click Add to then add this MAC address to the white list table.
Upload White List File	To upload a white list file, click Browse and navigate to the white list file, saved on the computer, and then click Upload .

Click the  icon to delete an existing entry.
 Click the **Save** button to accept the changes made.
 Click the **Back** button to discard the changes made and return to the main page.

Enable white list

MAC address: [Add](#)

Upload white list file: [Browse...](#) [Upload](#)

No.	MAC address	Delete
1	00:11:22:33:44:55	

[Save](#) [Back](#)

After selecting **Passcode** as the **Authentication Type**, we can view and configure the following section.

The following parameters can be configured.

Parameter	Description
Session timeout	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.
IP Address	Enter the IP address or network address that will be used in the IP filter rule here. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.
Subnet Mask	Enter the subnet mask of the IP address or networks address that will be filtered here. For example, 255.255.255.0.

Click the **Add** button to add the new IP filter rule.

Click the  icon to delete an existing rule.

User authentication

Authentication type: Passcode


Session timeout(1~1440) : 60 minute(s)

IP filter settings

IP address

Subnet mask

Add

IP address	Subnet mask	Delete	
192.168.70.150	255.255.255.0		

In this table configured front desk user accounts that have been assigned to this network and have already generated a pass code from the Web login page, will be displayed.

Passcode list							
Passcode	SSID	Duration	User limit	Last active day	Duration remaining	Creator	Status

CWM Configuration

Configuration

Site

Network

SSID

Create SSID

Parameter	Description
Web redirection	Select this option to enable the website redirection feature.
Website	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https:// , enter the URL of the website that will be used in the space provided.
Choose template	Select the login page that will be used here.

After selecting the style to use, click the **Preview** button to preview the selected style.

Click the **Upload login file** button to upload a new style.

Click the [Delete the style](#) link to delete the selected style.

Click the [Download Template](#) link to download the style template.

In the following section we can configure what network devices are allowed to connect to this network by specifying the MAC address of those network devices.


The following parameters can be configured.

Parameter	Description
Enable White List	Select this option to enable the white list feature.
MAC Address	Enter the MAC address of the networking device that will be allowed to connect to this network here. Click Add to then add this MAC address to the white list table.
Upload White List File	To upload a white list file, click Browse and navigate to the white list file, saved on the computer, and then click Upload .

Click the  icon to delete an existing entry.

Click the **Save** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the main page.

No.	MAC address	Delete
1	00:11:22:33:44:55	

For more information about creating or configuring user accounts refer to “**Create User Account**” on page 66.

For more information about front desk user accounts refer to “**Appendix A - Front Desk Staff & User Access**” on page 98.

CWM Configuration


Configuration


Site

Network

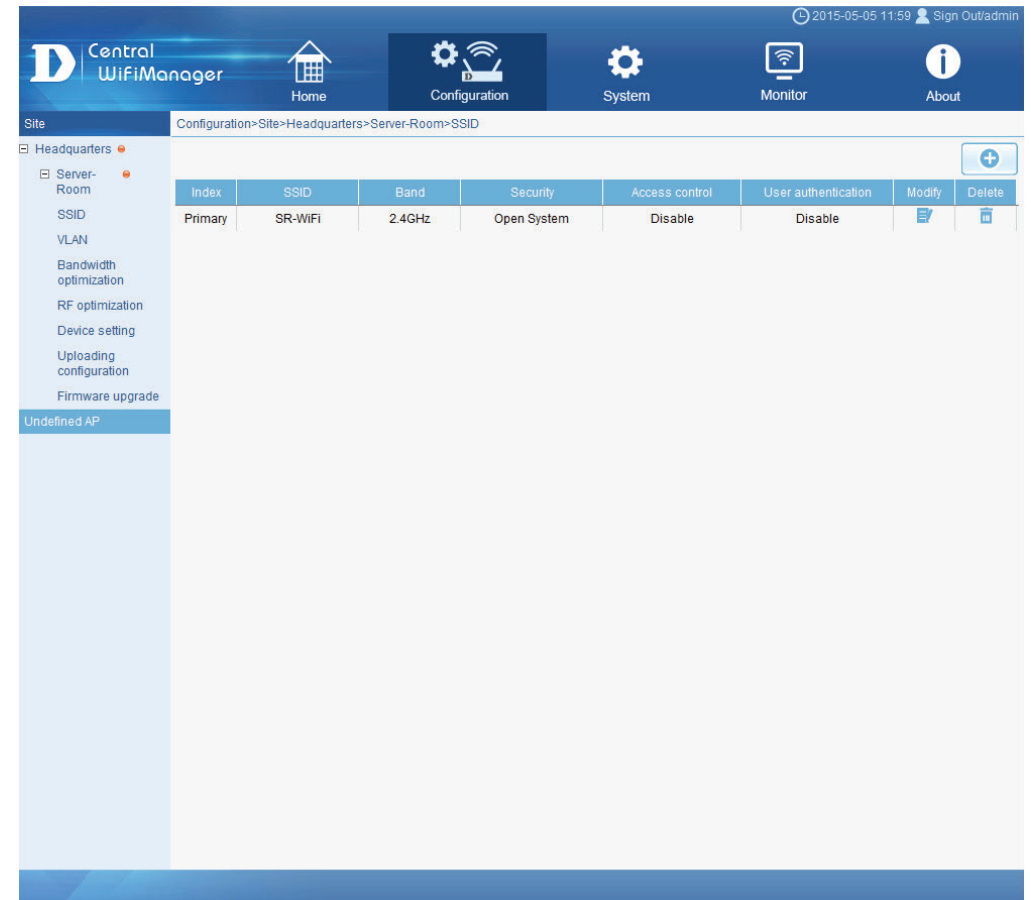
SSID

After creating a new SSID, it will be displayed in the table. In this example, we created an SSID called **SR-WiFi**.



Click the  button to add another new SSID.

Click the  icon to modify an existing SSID.

Click the  icon to delete an existing SSID.



The screenshot displays the Central WifiManager configuration interface. The top navigation bar includes the D-Link logo, the text "Central WifiManager", and several icons: Home, Configuration, System, Monitor, and About. The current page is titled "Configuration>Site>Headquarters>Server-Room>SSID". On the left, a sidebar menu shows a tree structure with "Headquarters" expanded to "Server-Room", which is further expanded to "SSID". Below the menu, a table lists the configured SSIDs. The table has columns for Index, SSID, Band, Security, Access control, User authentication, Modify, and Delete. A single row is visible with the following data:

Index	SSID	Band	Security	Access control	User authentication	Modify	Delete
Primary	SR-WiFi	2.4GHz	Open System	Disable	Disable		

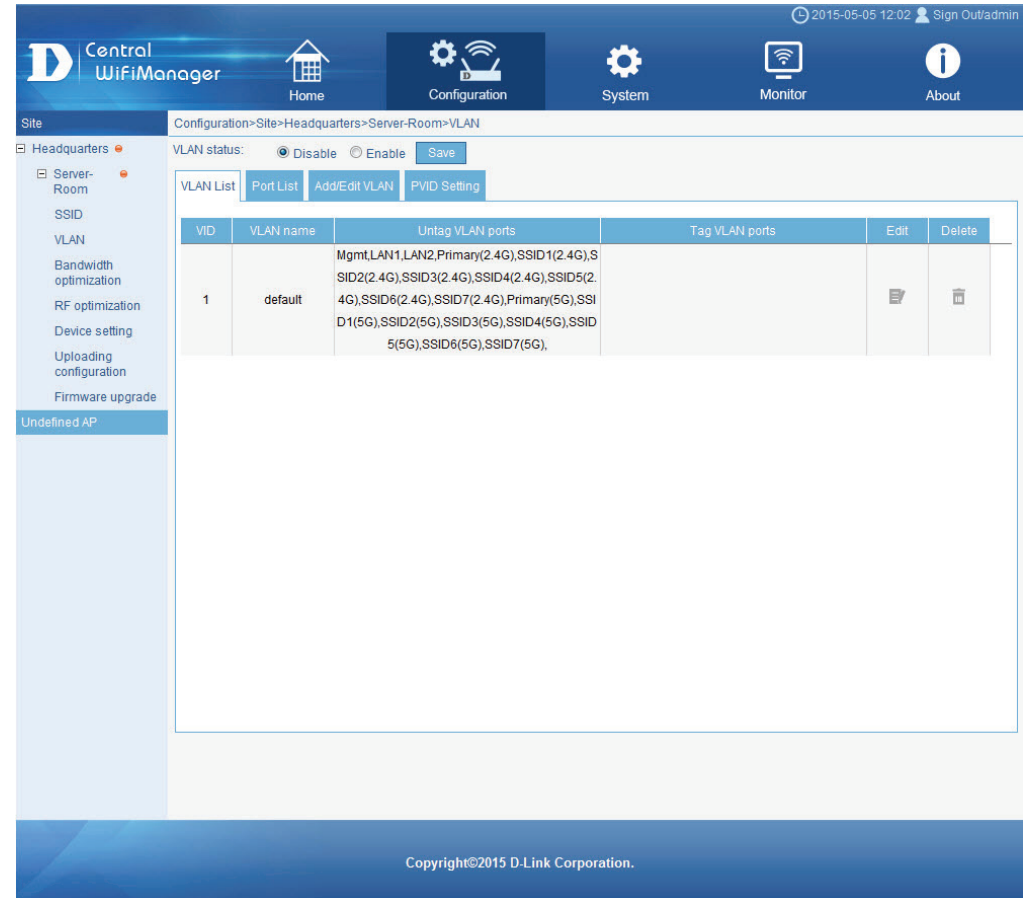
After creating a network, additional options will be available in the left panel. These options include **VLAN**, **Bandwidth Optimization**, **Captive Portal**, **RF Optimization**, **Device settings**, **Uploading Configuration** and **Firmware Upgrade**.

In the following sections, we'll discuss these additional settings in more detail.

Before the tabs, we can configure the following parameter.

Parameter	Description
VLAN Status	Select to Enable or Disable the VLAN feature here.

Click the **Save** button to accept the changes made.



CWM Configuration

Configuration

Site

Network

VLAN

After clicking on **VLAN** in the left panel, the following page will be available. On this page we can view, create and configure Virtual LANs (VLANs) that will be managed by the access point in this network.



In the **VLAN List** tab, a list of created VLANs will be displayed.

Click the **Edit** icon to modify an existing VLAN.

Click the **Delete** icon to remove an existing VLAN.

In the **Port List** tab, a list of ports will be displayed. These ports are all the ports that are available on the access points in the network.

In the columns next to the **Port Name** entries, the VLAN ID number of the VLAN that the port belongs to will be displayed. The column location of the number will indicate if the port is a tagged member (**Tag VID**) or an untagged member (**Untag VID**) of the VLAN. In the last column the **PVID** number of that specific port will be displayed.

VLAN List					
Port List					
Add/Edit VLAN					
PVID Setting					
VID	VLAN Name	Untag VLAN Ports	Tag VLAN Ports	Edit	Delete
1	default	Mgmt, LAN1, LAN2, Primary(2.4G), SSID1(2.4G), SSID2(2.4G), SSID3(2.4G), SSID4(2.4G), SSID5(2.4G), SSID6(2.4G), SSID7(2.4G), Primary(5G), SSID1(5G), SSID2(5G), SSID3(5G), SSID4(5G), SSID5(5G), SSID6(5G), SSID7(5G),			

VLAN List				
Port List				
Add/Edit VLAN				
PVID Setting				
Port Name	Tag VID	Untag VID	PVID	
Mgmt		1	1	
LAN1		1	1	
LAN2		1	1	
Primary(2.4G)		1	1	
Primary(5G)		1	1	
SSID1(2.4G)		1	1	
SSID2(2.4G)		1	1	
SSID3(2.4G)		1	1	
SSID4(2.4G)		1	1	
SSID5(2.4G)		1	1	
SSID6(2.4G)		1	1	
SSID7(2.4G)		1	1	
SSID1(5G)		1	1	
SSID2(5G)		1	1	
SSID3(5G)		1	1	
SSID4(5G)		1	1	
SSID5(5G)		1	1	
SSID6(5G)		1	1	
SSID7(5G)		1	1	

CWM Configuration

Configuration

Site

Network

VLAN

In the **Add/Edit VLAN** tab, we can create a new VLAN and assign the port membership to each port in that VLAN. After clicking the **Modify** icon in the **VLAN List** tab, we will be re-directed to this tab to modify an existing VLAN.

The following parameters can be configured.

Parameter	Description
VLAN ID (VID)	Enter the VLAN's ID here.
VLAN Name	Enter the VLAN's name here.
Port	Select the port membership option for each port in this column. Port in VLAN in this network can either be untagged (Untag) members, tagged (Tag), or non-members (Not Member).
Select All	Which this button is clicked, all the ports in the table will be changed to either be Untag , Tag or Not Member .
Mgmt	This is the management port on access points.
LAN1 ~ LAN2	This is the LAN ports on access points. If the access point has only one LAN port, it will be LAN1.
Primary	This is the primary WLAN SSID on access points in this network.
SSID1 ~ SSID7	This is the secondary WLAN SSIDs on access points in this network.

VLAN List
Port List
Add/Edit VLAN
PVID Setting

VLAN ID (VID)
 VLAN Name

Port	Select All	Mgmt	LAN1	LAN2
Untag	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.4GHz

MSSID Port	Select All	Primary	SSID1	SSID2	SSID3	SSID4	SSID5	SSID6	SSID7
Untag	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5GHz

MSSID Port	Select All	Primary	SSID1	SSID2	SSID3	SSID4	SSID5	SSID6	SSID7
Untag	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save

Click the **Save** button to accept the changes made.

CWM Configuration

Configuration

Site

Network

VLAN

In the **PVID Setting** tab, we can view and configure the Port VLAN Identifier (PVID) settings for access points and wireless client in this network.

The following parameters can be configured.

Parameter	Description
PVID Auto Assign Status	Select to Enable or Disable the PVID automatic assign status feature here.
PVID	Enter the PVID number in the spaces provided for the corresponding ports.
Mgmt	This is the management port on access points.
LAN1 ~ LAN2	This is the LAN ports on access points. If the access point has only one LAN port, it will be LAN1.
Primary	This is the primary WLAN SSID on access points in this network.
SSID1 ~ SSID7	This is the secondary WLAN SSIDs on access points in this network.

Click the **Save** button to accept the changes made.

VLAN List
Port List
Add/Edit VLAN
PVID Setting

PVID Auto Assign Status Disable Enable

Port	Mgmt	LAN1	LAN2
PVID	1	1	1

2.4GHz

MSSID Port	Primary	SSID1	SSID2	SSID3	SSID4	SSID5	SSID6	SSID7
PVID	1	1	1	1	1	1	1	1

5GHz

MSSID Port	Primary	SSID1	SSID2	SSID3	SSID4	SSID5	SSID6	SSID7
PVID	1	1	1	1	1	1	1	1

Save

CWM Configuration

Configuration

Site

Network

Bandwidth Optimization

After clicking on **Bandwidth Optimization** in the left panel, the following page will be available. On this page we can view and configure the bandwidth settings for access points in this network.

The following parameters can be configured.

Parameter	Description
Enable Bandwidth Optimization	Select to Enable or Disable the bandwidth optimization feature here.
Downlink Bandwidth	Enter the total downlink bandwidth speed for access points in this network here. This value is in Mbits/sec.
Uplink Bandwidth	Enter the total uplink bandwidth speed for access points in this network here. This value is in Mbits/sec.
Rule Type	Select the type of rule that will be create or modified here. Options to choose from are the following: <ul style="list-style-type: none"> • Allocate average BW for each station: The AP will distribute average bandwidth for each client. • Allocate maximum BW for each station: Specify the maximum bandwidth for each connected client. Reserve certain bandwidth for future clients. • Allocate different BW for 11a/b/g/n station: The weight of 802.11b/g/n and 802.11a/n clients are 10%/20%/70% and 20%/80%. The AP will distribute different bandwidth for 802.11a/b/g/n clients. • Allocate specific BW for SSID: All clients share the total bandwidth.
Band	Select the wireless frequency band that will be used in this rule here. Options to choose from are 2.4Ghz and 5GHz .
SSID	Select which SSID will be used in this rule here. Options to choose from are Primary SSID and SSID1 to SSID7 .
Downlink Speed	Enter the downlink speed value that will be assigned to either each station or to the specified SSID here. This value can either be in Mbits/sec or Kbits/sec .
Uplink Speed	Enter the uplink speed value that will be assigned to either each station or to the specified SSID here. This value can either be in Mbits/sec or Kbits/sec .


Click the **Add** button to add the new rule to the list of **Bandwidth Optimization Rules**.

The screenshot displays the 'Bandwidth optimization' configuration page. The left sidebar shows a tree view with 'Server-Room' selected. The main area contains the following settings:

- Enable bandwidth optimization:** A dropdown menu set to 'Disable'.
- Downlink bandwidth:** An input field with 'Mbits/sec' unit.
- Uplink bandwidth:** An input field with 'Mbits/sec' unit.
- Add bandwidth optimization rule:** A section with a dropdown for 'Rule type' (set to 'Allocate average bandwidth for each station'), a 'Band' dropdown (set to '2.4 GHZ'), an 'SSID' dropdown (set to 'PrimarySSID'), and input fields for 'Downlink speed' and 'Uplink speed' (both with 'Mbits/sec' units). 'Add' and 'Clear' buttons are present.
- Bandwidth optimization rules:** A table with columns: Band, Type, SSID, Downlink speed, Uplink speed, Modify, Delete. The table is currently empty.

A 'Save' button is located at the bottom right of the configuration area. The footer of the page reads 'Copyright©2015 D-Link Corporation.'

Click the **Clear** button to clear out all the information entered in the fields. Click the **Save** button to accept the changes made.

Click the  icon to modify an existing rule.

Click the  icon to delete an existing rule.

CWM Configuration

Configuration

Site

Network

RF optimization

After clicking on **RF** in the left panel, the following page will be available. On this page we can view and optimize the Radio Frequency (RF) used on the access points in this network.

The following parameters can be configured.

Parameter	Description
Enable Auto RF	Select this option to enable the RF optimization feature.
Init Auto RF	Click the Auto RF Optimize button to manually initiate the automatic RF optimization feature. The AP will automatically select the best channel.
Auto Init	Select this option to run the RF optimization feature periodically based on the period entered. After the initiation period has expired, the AP will automatically select the best channel.
Auto Init Period	After enabling the Auto Init option, enter the automatic initiation period value in hours here.
RSSI Threshold	Select the RSSI threshold value for this network here. This value is between 10% and 100% in increments of 10%. The AP will adjust its channel or power when, after a scan, it detected APs in the network with a lower RSSI than the threshold specified.
RF Report Frequency	Enter the frequency value, in seconds, at which an RF report will be generated. The AP might adjust its channel or power at the frequency specified.

Click the **Save** button to accept the changes made.

The screenshot shows the 'RF optimization' configuration page in the Central WifiManager. The breadcrumb trail is 'Configuration > Site > Headquarters > Server-Room > RF optimization'. The left sidebar shows a tree view with 'Server-Room' selected. The main content area contains the following settings:

- Enable auto RF:**
- Initiate auto RF:** [Auto RF Optimize](#)
- Auto initiation:**
- Auto initiation period:** 24 (Hours)
- RSSI threshold:** 40%
- RF report frequency:** 10 (Seconds)

A **Save** button is located at the bottom right of the configuration area. The footer of the page reads 'Copyright©2015 D-Link Corporation.'

CWM Configuration

Configuration

Site

Network

Device Settings

After clicking on **Device Settings** in the left panel, the following page will be available. On this page we can view and configure the login and accessibility settings for access points in this network. Additionally some advanced wireless settings can be configured on this page for both the 2.4Ghz and 5Ghz frequency bands.

The following parameters can be configured.

Parameter	Description
Username	This field displays the username that is applied to all access points in this network.
Password	Enter the password that will be applied to all access points in this network here.
Status	Select this option to enable console port connectivity on all access points in the network.
Console Settings	Select the console port protocol that will be used on all access points in this network. Options to choose from are Telnet and SSH .
Time Out	Select the active console session time out value here. Options to choose from are 1 Min , 3 Mins , 5 Mins , 10 Mins , 15 Mins , and Never .
External syslog server	Enter the IP address or domain name to save the Internet access services information for EU directive.
Choose Band	Select this option to choose the wireless band for DAP-2553.

Click the **Save** button to accept the changes made.

The screenshot displays the 'Device setting' page in the Central WifiManager interface. The breadcrumb trail is 'Configuration>Site>Headquarters>Server-Room>Device setting'. The left sidebar shows a tree view with 'Server-Room' selected. The main content area is divided into several sections:

- Admin:** Username: admin, Password: [redacted]
- Console settings:** Status: Enable, Console protocol: Telnet SSH, Time out: 3 Mins
- Automatic Time Configuration:** Enable NTP Server: [unchecked], NTP Server: [redacted], Time Zone: (GMT-05:00) Eastern Time (US & Canada), Enable Daylight Saving: [unchecked]
- External syslog server:** [redacted] (IP address/Domain name)
- Choose Band:** 2.4GHz (Take effect only for DAP-2553)
- 2.4GHz Wireless Settings:**
 - Data rate: Auto
 - RTS length (256-2346): 2346
 - Beacon interval (40-500): 100
 - Fragment length (256-2346): 2346
 - DTIM (1-15): 1
 - Wireless: On
 - Channel width: Auto 20/40 MHz

A 'Save' button is located at the bottom right of the configuration area. The footer of the page reads 'Copyright©2015 D-Link Corporation.'

CWM Configuration

Configuration

Site

Network

Device Settings

In the **2.4GHz** and **5GHz** sections the following parameters can be configured.

Parameter	Description
Data Rate	Select the wireless data rate that will be given the highest priority here. This rate is between 1 and 54 Mbps. Select Auto to allow the access point to determine the best rate.
RTS Length	Enter the RTS length value here. This value must be between 256 and 2346. By default, this value is 2346.
Beacon Interval	Enter the beacon interval value here. This value must be between 40 and 500. By default, this value is 100.
Fragment Length	Enter the fragment length value here. This value must be between 256 and 2346. By default, this value is 2346.
DTIM	Enter the DTIM value here. This value must be between 1 and 15. By default, this value is 1.
Wireless	Select whether the wireless connectivity of access points in this network should be On or Off .
11N Channel Width	Select the 802.11n wireless channel width here. Options to choose from are 20 MHz and Auto 20/40 MHz . In the 5GHz section, an additional Auto 20/40/80 MHz option is available for selection.

In the **5GHz** section the following additional parameters can be configured.

Parameter	Description
Band Steering Age	Enter the band steering age value here. This value must be between 0 and 600. By default, this value is 180.
Band Steering Difference	Enter the band steering difference value here. This value must be between 0 and 32. By default, this value is 2.
Band Steering Refuse Number.	Enter the band steering refuse number here. This value must be between 0 and 10. By default, this value is 3.

2.4GHz | 5GHz

Data Rate

RTS Length (256-2346)

Beacon Interval (40-500)

Fragment Length (256-2346)

DTIM (1-15)

Wireless

11N Channel Width

2.4GHz | 5GHz

Data Rate

RTS Length (256-2346)

Beacon Interval (40-500)

Fragment Length (256-2346)

DTIM (1-15)

Wireless

11N Channel Width

Band Steering

Band Steering Age(0-600)

Band Steering Difference(0-32)

Band Steering Refuse Number(0-10)

After clicking on **Uploading Configuration** in the left panel, the following page will be available. On this page we can view and configure the configuration file upload schedule or initiate the upload of the configuration file to all access points in this network manually.

In the **Schedule Settings** section, the following parameters can be configured.

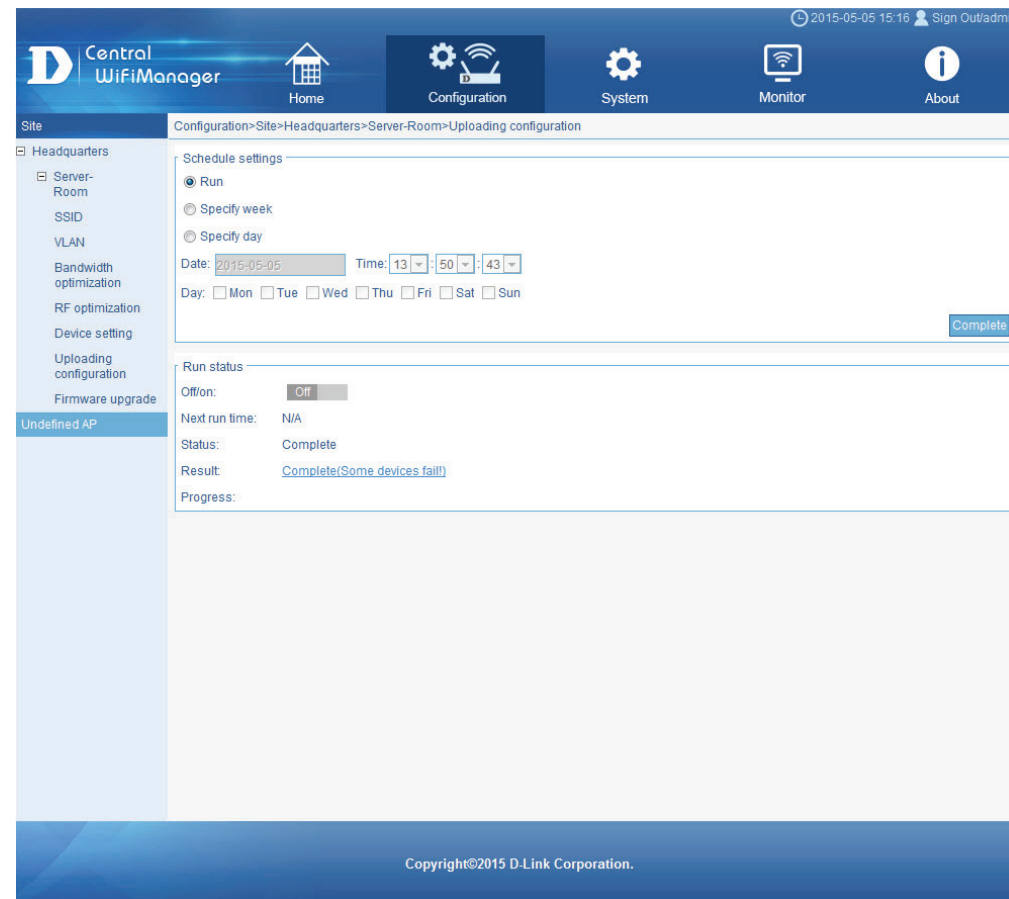
Parameter	Description
Run	Select this option to manually upload the configuration file to all the access points in this network manually. Click Complete to initiate the upload.
Specify Time	Select this option to configure the scheduled time for the configuration upload to take place. Selecting this option will initiate the configuration upload every weekday specified at the time specified continuously.
Specify Date	Select this option to configure the scheduled date for the configuration upload to take place. Selecting this option will only initiate the configuration upload once on the date and time specified.
Date	After selecting the Specify Date option, select the date at which the upload will be initiated.
Time	After selecting the Specify Time or the Specify Date option, select the time at which the upload will be initiated.
Day	After selecting the Specify Time option, select the day(s) on which the upload will be initiated.

Click the **Complete** button to accept the changes made or to manually initiate the upload.

In the **Run Status** section, the following parameters can be configured.

Parameter	Description
Off/On	Toggle this option to On , to enable the scheduled configuration upload configured. Toggle this option to Off to disable the scheduled upload. To reconfigure the schedule settings, this option must be turned off.

After the first upload, the **Next Run Time** field will display when the next upload will take place. After every upload, the **Result** hyperlink will be made available for review.



CWM Configuration

Configuration

Site

Network

Firmware Upgrade

After clicking on **Firmware Upgrade** in the left panel, the following page will be available. On this page we can view and configure the firmware file upload schedule or initiate the upload of the firmware file to all access points in this network manually.

In the **Choose Firmware** section, the following parameters can be configured.

Parameter	Description
Firmware File	For every access point in this network, we can specify the firmware file that will be uploaded either manually, or based on the schedule configured. Click Browse to navigate to the firmware file located on the computer.

In the **Schedule Settings** section, the following parameters can be configured.

Parameter	Description
Run	Select this option to manually upload the firmware file to all the specified access points in this network manually. Click Complete to initiate the upload.
Specify Time	Select this option to configure the scheduled time for the firmware upload to take place. Selecting this option will initiate the firmware upload every weekday specified at the time specified continuously.
Specify Date	Select this option to configure the scheduled date for the firmware upload to take place. Selecting this option will only initiate the firmware upload once on the date and time specified.
Date	After selecting the Specify Date option, select the date at which the upload will be initiated.
Time	After selecting the Specify Time or the Specify Date option, select the time at which the upload will be initiated.
Day	After selecting the Specify Time option, select the day(s) on which the upload will be initiated.

Click the **Complete** button to accept the changes made or to manually initiate the upload.

The screenshot displays the 'Firmware Upgrade' configuration interface. At the top, there's a navigation bar with 'Home', 'Configuration', 'System', 'Monitor', and 'About' buttons. The main content area is titled 'Configuration > Site > Headquarters > Server-Room > Firmware upgrade'. On the left, a sidebar menu lists various settings like 'Server-Room', 'SSID', 'VLAN', 'Bandwidth optimization', 'RF optimization', 'Device setting', 'Uploading configuration', and 'Firmware upgrade'. The 'Firmware upgrade' section is active, showing a 'Choose firmware' table with columns for 'Module name', 'Module version', 'Hardware version', 'Current firmware file', and 'Firmware file'. Below the table, the 'Schedule settings' section has three radio buttons: 'Run' (selected), 'Specify week', and 'Specify day'. The 'Run' option is selected, and the date is set to '2015-05-05' and the time is '15:19:19'. There are checkboxes for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). A 'Complete' button is visible. The 'Run status' section shows 'Off/on: Off', 'Next run time:', 'Status:', 'Result:', and 'Progress:'.

CWM Configuration

Configuration

Site

Network

Firmware Upgrade

In the **Run Status** section, the following parameters can be configured.

Parameter	Description
Off/On	Toggle this option to On , to enable the scheduled firmware upload configured. Toggle this option to Off to disable the scheduled upload. To reconfigure the schedule settings, this option must be turned off.

After the first upload, the **Next Run Time** field will display when the next upload will take place. After every upload, the **Result** hyperlink will be made available for review.

The screenshot displays the Central WifiManager interface for configuring the firmware upgrade process. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar shows a tree view with 'Firmware upgrade' selected under 'Server-Room'. The main content area is titled 'Configuration>Site>Headquarters>Server-Room>Firmware upgrade' and contains the following sections:

- Choose firmware:** A table with columns for 'Module name', 'Module version', 'Hardware version', 'Current firmware file', and 'Firmware file'.
- Schedule settings:** Radio buttons for 'Run' (selected), 'Specify week', and 'Specify day'. Below are date and time pickers (Date: 2016-05-05, Time: 15:19:19) and a 'Day' selection row with checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun.
- Run status:** A section with an 'Off' toggle, and fields for 'Next run time:', 'Status:', 'Result:', and 'Progress:'.


A 'Complete' button is visible at the bottom right of the 'Schedule settings' section. The footer of the page reads 'Copyright©2015 D-Link Corporation.'

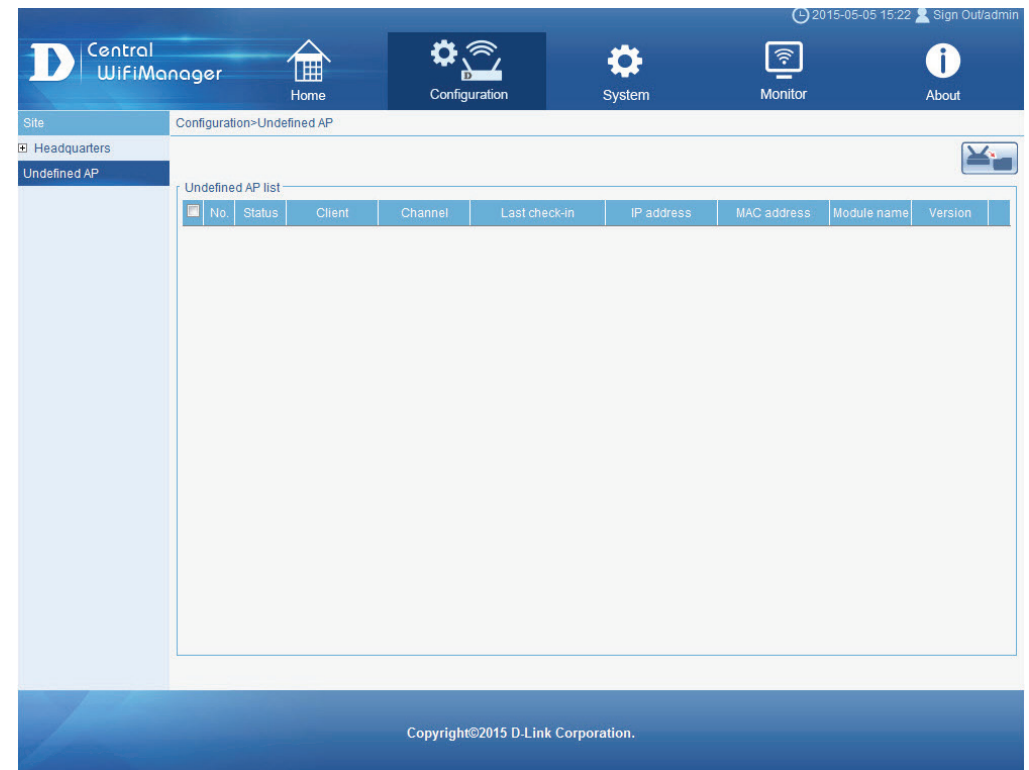
CWM Configuration

Configuration

Undefined AP

After clicking on **Undefined AP** in the left panel, the following page will be available. On this page we can view a list of access points that do not belong to a network configured in any site.

To add an access point in this list to a network, select the check box next to the entry and click the  icon on the top, right of this page. A list of available networks will be displayed that can be selected for the move.



The screenshot shows the D-Link Central WifiManager Configuration page. The top navigation bar includes the D-Link logo, "Central WifiManager", and icons for Home, Configuration, System, Monitor, and About. The current page is "Configuration > Undefined AP". The left sidebar shows "Site" with "Headquarters" and "Undefined AP" listed. The main content area displays an "Undefined AP list" table with the following columns: No., Status, Client, Channel, Last check-in, IP address, MAC address, Module name, and Version. The table is currently empty. The footer of the page reads "Copyright©2015 D-Link Corporation."

CWM Configuration System Settings **General**

On this page we can view and configure settings that are related to the system functionality of the Central WifiManager application.

In the following sections we will discuss these settings in more detail.

After clicking on **System** in the top panel and **Settings** in the left panel, the following page will be displayed. On this page there are five tabs with various settings that can be configured. They are **General**, **Module**, **Database**, **Advance** and **SMTP**.

In the **General** tab, the following parameters can be configured.

Parameter	Description
Save Your Login Settings	In the Login Settings section, select this option to choose whether the login session should be remembered or not. After selecting the None option, the user will be prompt to login every time a connection to the Web User Interface (Web UI) is made. After selecting the 1 week option, the user session will be kept open for one week. During this time, the user will not be asked to login again after the initial login was made except if the user manually logged out.
Max. Online User	In the Login Settings section, enter the maximum amount of users that will be allowed to access the management interface at the same time. This value must be between 1 and 10. By default, this value is 5.
Live packet interval time	In the AP List Packet Settings section, select the live packet interval time here. Options to choose from are Auto , 2 , 5 , 10 , 20 , and 30 .
Time Zone	In the Time Zone Settings section, select the correct time zone option here.
Access Address	In the Connection Settings section, enter the Central WifiManager Server application's IP address here.
Listen Port	In the Connection Settings section, enter the Central WifiManager Server application's listen port number here. By default, this value is 8090.
Service Port	In the Connection Settings section, enter the Central WifiManager Server application's service port number here. By default, this value is 64768.

Click the **OK** button to accept the changes made.

The screenshot displays the 'System-Settings' page in the Central WifiManager application. The 'General' tab is active, showing the following settings:

- Login settings:** 'Save your login settings' is set to 'None'. 'Maximum online users' is set to 5 (with a note 'Maximum number is 10').
- AP live packet settings:** 'Live packet interval time' is set to 'Auto' (Seconds).
- Time zone setting:** 'Time zone' is set to '(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi'.
- Connection setting:** 'Access address' is 'ec2-54-214-48-226.us-west-2.com'. 'Listening port' is 8090 and 'Service port' is 64768. A red warning message indicates: 'Server must be restarted for changes in settings to take effect.'

An 'OK' button is located at the bottom right of the settings area.

CWM Configuration System Settings **Module**

In the **Module** tab, a list of access point modules will be displayed in the **Module Name** section. Every different model of access point that will be managed by the Central WifiManager Server application, requires the administrator to install the executable module file for that specific access point's model name.


For example, on this page we have two kinds of access point modules installed, the DAP-2330 and the DAP-2660. This means that we can have multiple DAP-2330 and DAP-2660 access points installed on the network, but only required to install two modules. One for each type of access point.

NOTE: The module executable files for all the access points, supported in the application, can be downloaded from the D-Link website.

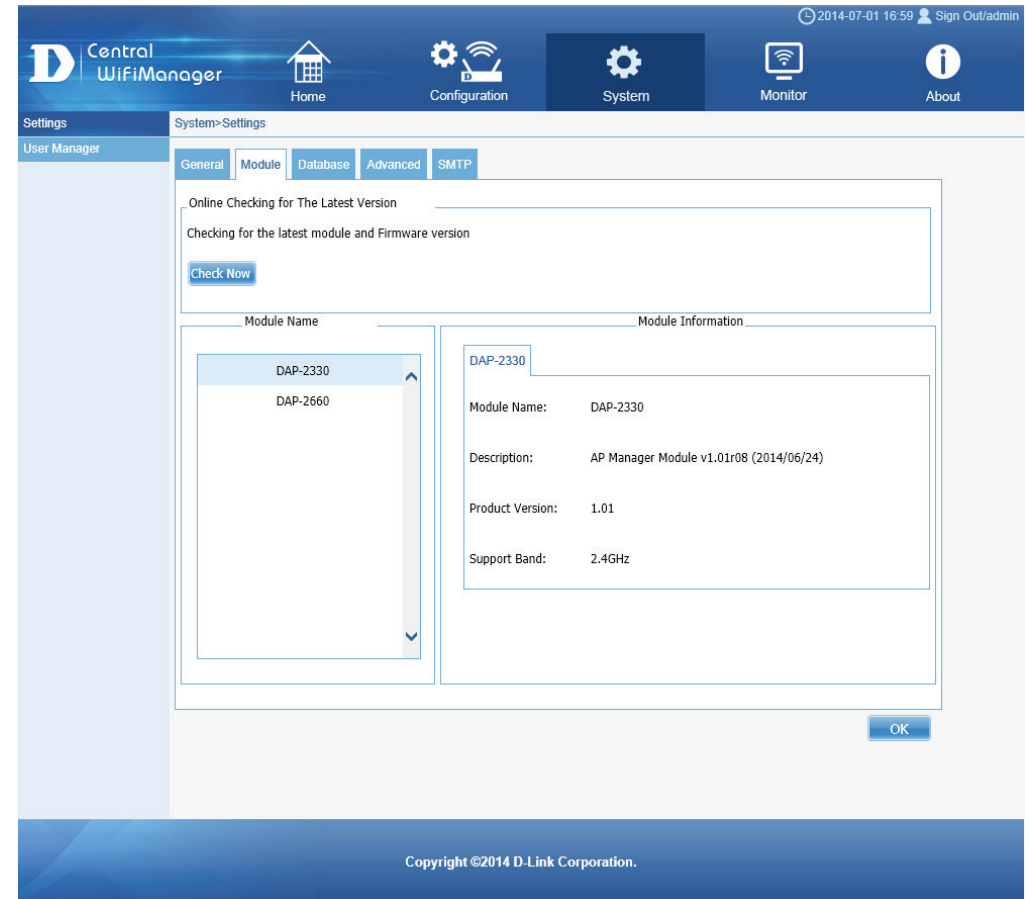
More information about the installed access point modules can be found in the **Module Information** section.

To keep the installed modules and firmware versions for access points up to date, click on the **Check Now** button.

Click the **OK** button to accept the changes made.

Online Check Version						
	Model Name	HW	Version	Result	Download	
	DAP-2330	A	1.01			
	DAP-2660	A	1.05			

After clicking on **Check Now**, the following page will be available. On this page the application will check if the installed access point modules are up to date.



Copyright ©2014 D-Link Corporation.

CWM Configuration

System

Settings

Database

After clicking on the **Database** tab, the following page will be available. On this page we can view and configure how this application backs up or restores the database information and at what time intervals this should take place. In the **Database** tab, there are two sub-tab pages called **General** and **Backup**.

In the **General** sub-tab, the following parameters can be configured.

Parameter	Description
Enable auto backup	Select this option to enable the automatic backup feature of the application's database.
Auto backup interval time	Enter the automatic backup interval time, in days, here. By default, this value is 7 days. To remove the old database backed up information after the new database was successfully backed up, select the ' Old data will be deleted once the automatic backup process finishes ' option and enter the pending days value in the text box. By default, this value is 7 days.
Data backup directory	In this field the path to the backup directory will be displayed for reference.

Click the **OK** button to accept the changes made.

The screenshot displays the configuration interface for the Database Backup settings. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The 'System-Settings' page is open, with the 'Database' tab selected. The 'Backup' sub-tab is active, showing the following configuration options:

- Enable auto backup:** (checked)
- Auto backup interval time:** 7 Days
- Old data will be deleted once the automatic backup process finishes:** (checked) 7 Days
- Data backup directory:** \\Server\WAPP_DATA\W-D-Link

An 'OK' button is located at the bottom right of the configuration area. The footer of the page reads 'Copyright©2014 D-Link Corporation.'

CWM Configuration

System

Settings

Database

In the **General** sub-tab, the following parameters can be configured.

Parameter	Description
Backup	In this section we can manually backup the system data to the computer accessing the Web interface. Click Backup Now to initiate the manual backup. The backup file is a PostgreSQL file with the file extension of SQL.
Restore	In this section we can manually navigate to a backed up file and restore those settings to this application. Click Browse and navigate to the previously backed up SQL file and then click Restore Now to initiate the restore.

Click the **OK** button to accept the changes made.

The screenshot displays the 'System-Settings' window with the 'Backup' sub-tab selected. The main content area contains the following text and controls:

- Header: "You can backup system data as well as restore from a previously saved one here"
- Section: "Backup"
 - Text: "Backup to local hard drive"
 - Button: "Backup Now" (highlighted in blue)
- Section: "Restore"
 - Text: "Choose backup file" followed by a file selection button and "(limit to 500M)"
 - Button: "Restore Now"

An "OK" button is located at the bottom right of the settings panel. The footer of the application reads "Copyright©2014 D-Link Corporation."

CWM Configuration System Settings **Advanced**

After clicking on the **Advanced** tab, the following page will be available. On this page we can view and configure advanced time settings for some features hosted by this application.

The following parameters can be configured.

Parameter	Description
Set timeout	Enter the maximum time allowed for settings to be made in this application. This is the time from the click of a button until the request was received by the server. By default, this value is 5 seconds.
Reboot time	Enter the time the Web application will wait after a reboot request was send by the server to access points. By default, this value is 50 seconds.
Configuration update time	Enter the time the Web application will wait after a configuration file update was initiated to access points by the server. By default, this value is 60 seconds.
Factory reset time	Enter the time the Web application will wait after a factory reset was initiated to access points by the server. By default, this value is 60 seconds.
FW download time	Enter the time the Web application will allow for firmware downloads initiated by the firmware update check feature. By default, this value is 80 seconds.
FW flash time	Enter the time the Web application will wait after a firmware flash update was initiated by the server to access points. By default, this value is 300 seconds.
Timing tolerance time	Enter the timing tolerance time value here. By default, this value is 5 seconds.

Click the **OK** button to accept the changes made.

The screenshot displays the 'Advanced' settings page for the Central WifiManager. The page is titled 'System-Settings' and includes a navigation menu with tabs for 'General', 'Module', 'Database', 'Advanced', and 'SMTP'. The 'SMTP' tab is currently selected. The configuration area is divided into several sections:

- Configuration server settings:** Includes fields for 'E-mail server', 'Port' (set to 25), and 'Encryption' (with checkboxes for SSL and TLS, and a 'Connect' button).
- Enable authentication:** A checkbox option with fields for 'Username' and 'Password'.
- E-mail settings:** Fields for 'From address', 'From name', 'Reply address', 'Reply name', and 'Word wrap' (set to 80).
- E-mail test:** A field for 'E-mail address' and a 'Test' button.

An 'OK' button is located at the bottom right of the configuration area. The footer of the page reads 'Copyright©2014 D-Link Corporation.'

CWM Configuration

System

Settings

SMTP

After clicking on the **SMTP** tab, the following page will be available. On this page we can view and configure the Simple Mail Transfer Protocol (SMTP) settings.

In the **Configure Server Settings** section, the following parameters can be configured.

Parameter	Description
Mail Server	Enter the SMTP server's IP address or domain name here.
Port	Enter the SMTP server's port number here. By default, this value is 25.
Encryption	If applicable, select the SMTP connection's encryption method here. Options available are SSL and TSL . Click Connect to test if the mail server settings are correct.
Enable authentication	Select this option if the SMTP server requires authentication to successfully send emails.
Username	After authentication was enabled, enter the SMTP user account's username here.
Password	After authentication was enabled, enter the SMTP user account's password here.

In the **Mail Settings** section, the following parameters can be configured.

Parameter	Description
From address	Enter the sender's email address here so that the recipient can recognize who is sending the email.
From name	Enter the sender's name here.
Reply address	Enter the recipient's email address here.
Reply name	Enter the recipient's name here.
Word wrap	Enter the word wrap value here. By default, this value is 80.

In the **Mail Test** section, the following parameters can be configured.


Parameter	Description
Mailbox address	To test if the recipient's email address is active, enter the recipient's email address here and click Test .

Click the **OK** button to accept the changes made.

CWM Configuration System User Manager

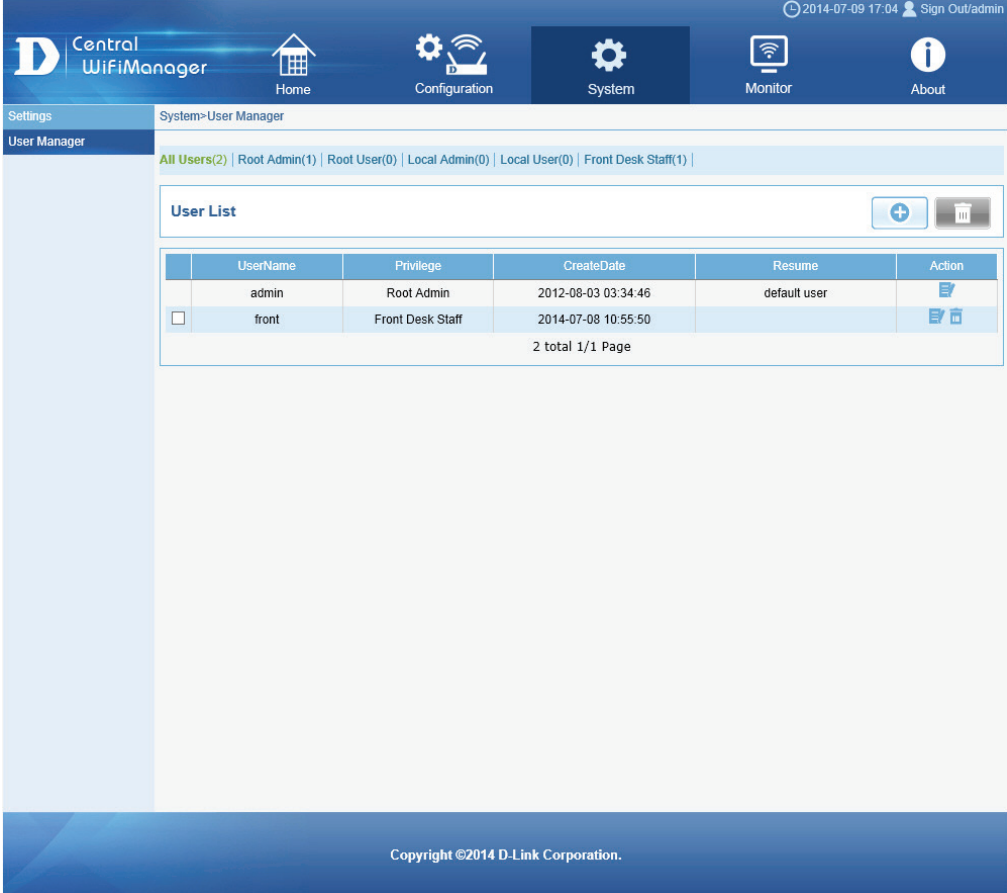
After clicking on **System** in the top panel and **User Manager** in the left panel, the following page will be displayed. On this page we can view, create and configure user accounts. There are five kinds of user accounts that can be created to access the Central WifiManager Server application.

In the **User List** section, a list of user accounts will be displayed.

Click the  button to add a new user account.

Click the  icon to modify an existing user account.

Click the  icon to delete an existing user account.






2014-07-09 17:04 Sign Out/admin

Central WifiManager Home Configuration System Monitor About

Settings System>User Manager

User Manager All Users(2) | Root Admin(1) | Root User(0) | Local Admin(0) | Local User(0) | Front Desk Staff(1)

User List

	UserName	Privilege	CreateDate	Resume	Action
	admin	Root Admin	2012-08-03 03:34:46	default user	
<input type="checkbox"/>	front	Front Desk Staff	2014-07-08 10:55:50		 

2 total 1/1 Page

Copyright ©2014 D-Link Corporation.

CWM Configuration

System

User Manager

Create User Account

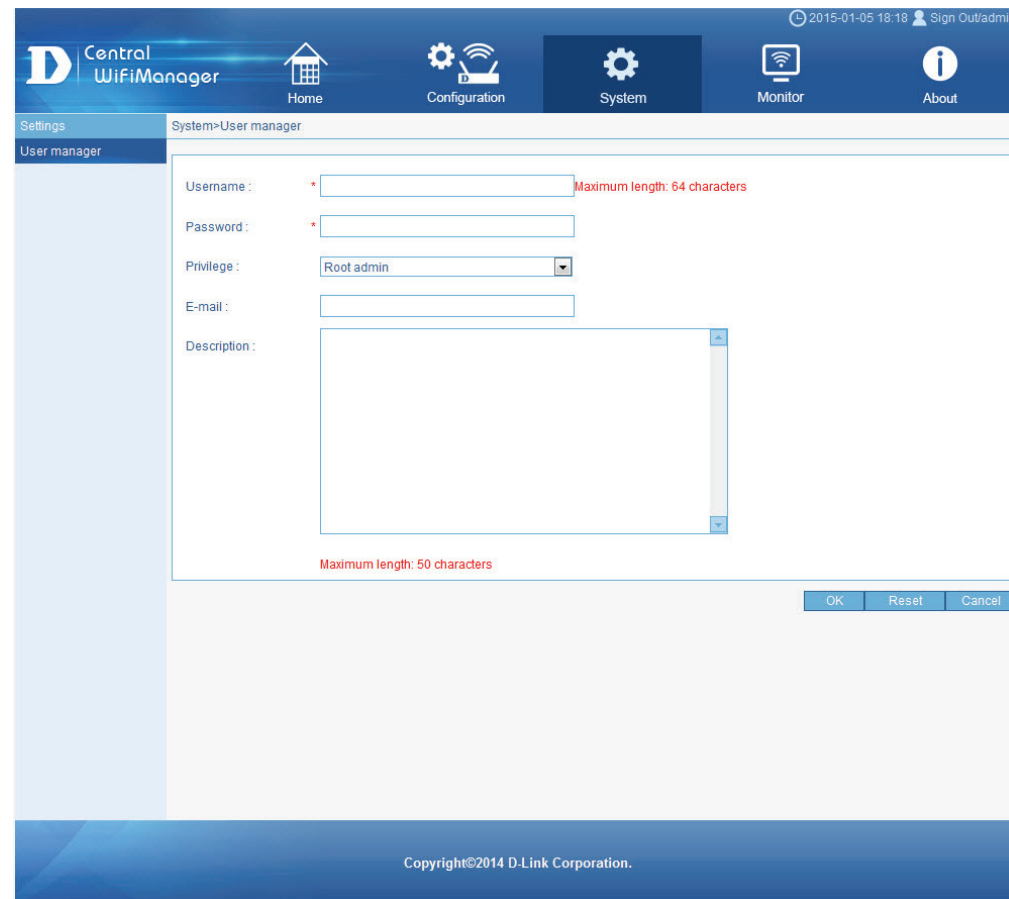
After clicking the  icon, the following page will be available. On this page we can configure the following parameters.

Parameter	Description
Username	Enter the username for the new user account here. This name must be between 4 and 64 characters long.
Password	Enter the password for the new user account here. This password must be between 4 and 64 characters long.
Privilege	Select the privilege level that this user account will have. Options to choose from are Root Admin, Root User, Local Admin, Local User, and Front Desk Staff.
E-mail	Enter the email address that will be associated with this user account here.
Description	Enter a more detailed description for this user account here.

Click the **OK** button to create the user account.

Click the **Reset** button to clear the information entered in the fields of this form.

Click the **Cancel** button to discard the changes made and return to the main page.



Central WifiManager

Home Configuration System Monitor About

Settings System>User manager

User manager

Username : * Maximum length: 64 characters

Password : *

Privilege :

E-mail :

Description :

Maximum length: 50 characters

OK Reset Cancel

Copyright©2014 D-Link Corporation.

CWM Configuration

Monitor


Report

Association

By Access Point


After clicking on **Monitor** in the top panel and **Association** in the left panel, the following page will be displayed. On this page we can view a report of all the access points and wireless clients managed by this application. Three association reports can be generated **By Access Point**, **By Wireless Station**, and **By Station Number**.

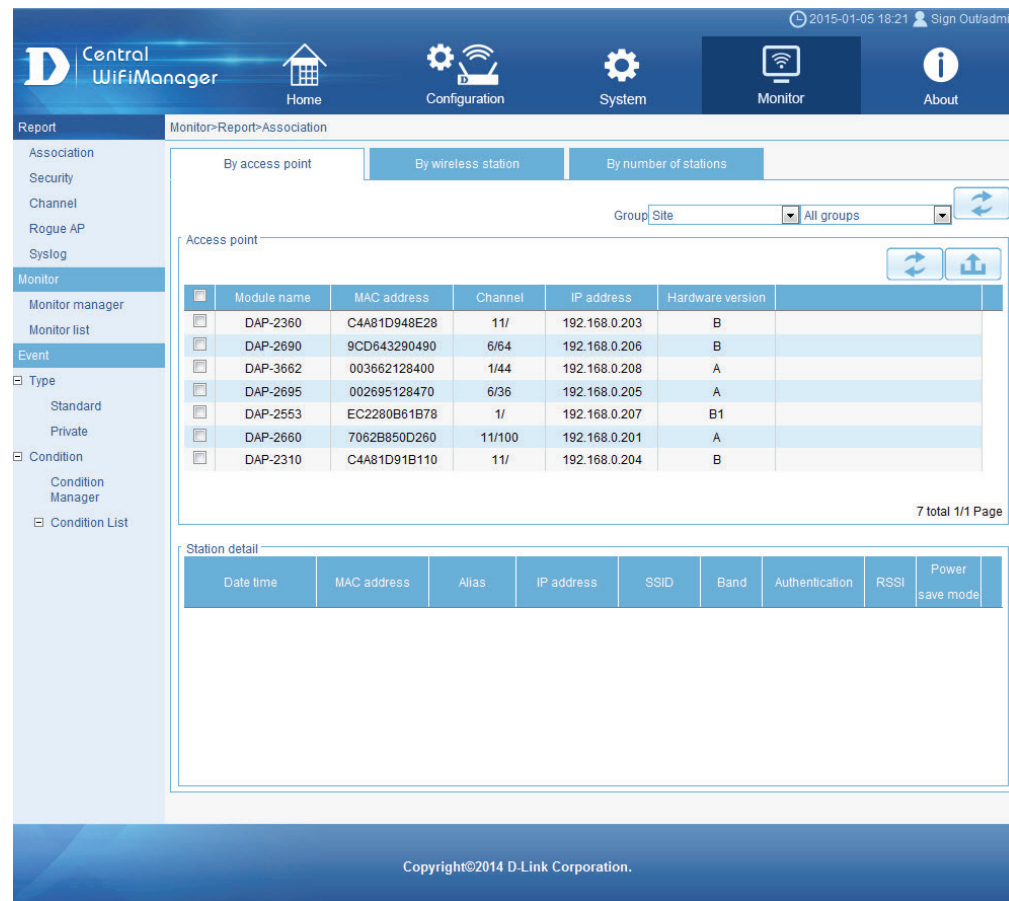
On this page a report was generated **By Access Point**. This report can be refined by selecting the **Group** (Site), from the first drop-down menu, and also then selecting the network in the second drop-down menu.

Click the  button to regenerate this report.

In the **Access Point** table the list of access points, managed by this application, will be displayed. Information like the **Module Name**, **MAC Address**, **Channel**, **IP Address** and **HW Version** is displayed for each access point.

In the **Station Detail** table the list of wireless clients, connected to the access points, managed by this application, will be displayed. Information like **Date/Time**, **MAC Address**, **Alias**, **IP Address**, **SSID**, **Band**, **Authentication**, **RSSI** and **Power Save Mode** is displayed for each wireless client.

Click the  button to export the contents displayed in these tables to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot displays the Central WifiManager web interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar shows a menu with 'Report' selected, and 'Association' highlighted. The main content area shows the 'Monitor-Report>Association' page with three tabs: 'By access point', 'By wireless station', and 'By number of stations'. The 'By access point' tab is active, showing a table of access points. The table has columns for Module name, MAC address, Channel, IP address, and Hardware version. Below the table, there is a 'Station detail' section with a table for wireless clients, including columns for Date time, MAC address, Alias, IP address, SSID, Band, Authentication, RSSI, and Power save mode. The interface also includes a 'Group' dropdown menu set to 'Site' and 'All groups', and a '7 total 1/1 Page' indicator.

Module name	MAC address	Channel	IP address	Hardware version
DAP-2360	C4A81D948E28	11/	192.168.0.203	B
DAP-2690	9CD643290490	6/64	192.168.0.206	B
DAP-3662	003662128400	1/44	192.168.0.208	A
DAP-2695	002695128470	6/36	192.168.0.205	A
DAP-2553	EC2280B61B78	1/	192.168.0.207	B1
DAP-2660	7062B850D260	11/100	192.168.0.201	A
DAP-2310	C4A81D91B110	11/	192.168.0.204	B

Date time	MAC address	Alias	IP address	SSID	Band	Authentication	RSSI	Power save mode

Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor

Report


Association

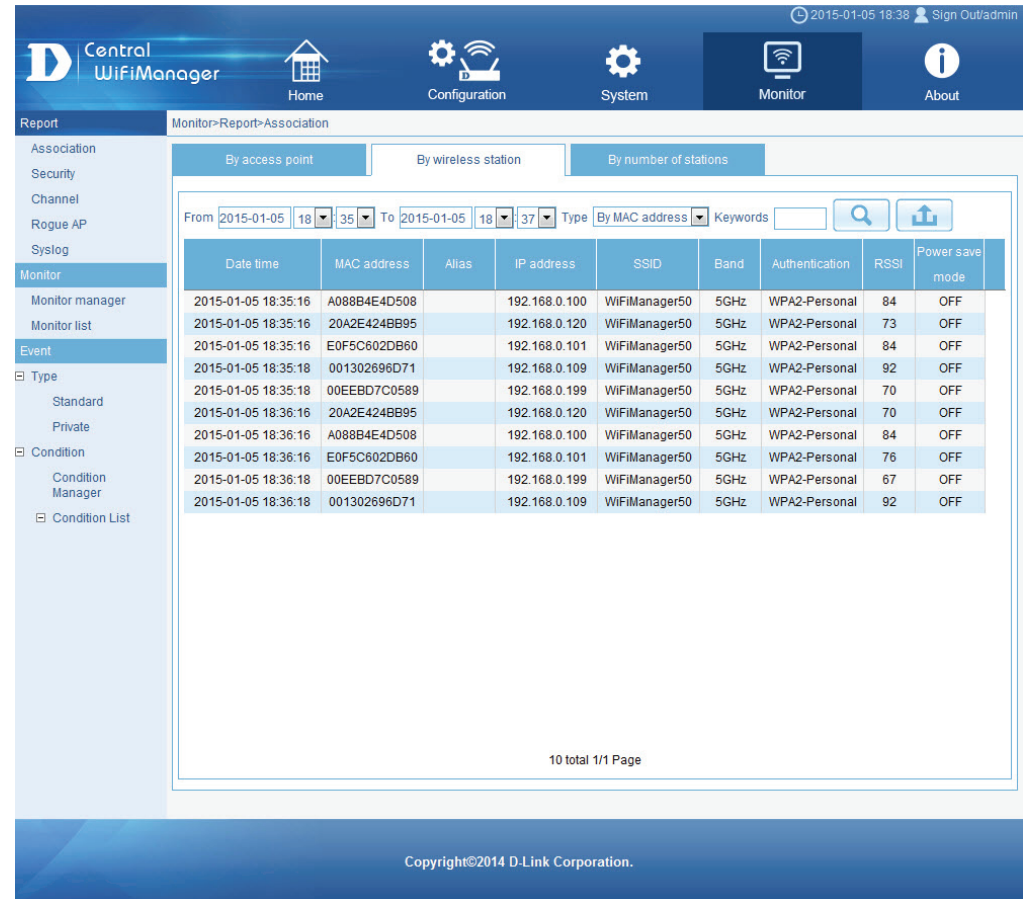
By Wireless Station

On this page a report was generated **By Wireless Station**. This report can be refined by selecting the date and time **From** and **To**, and then selecting the **Type**, either **By MAC Address** or **By Alias**, and also additionally entering **Key Words** in the text box provided.

Click the  button to regenerate this report.

In the table a list of wireless client connections, connected to the access points, managed by this application, will be displayed. Information like **Date/Time**, **MAC Address**, **Alias**, **IP Address**, **SSID**, **Band**, **Authentication**, **RSSI** and **Power Save Mode** is displayed for each wireless client.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot shows the Central WifiManager web interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar contains 'Report', 'Association', 'Security', 'Channel', 'Rogue AP', 'Syslog', 'Monitor', 'Monitor manager', 'Monitor list', 'Event', 'Type', 'Standard', 'Private', 'Condition', 'Condition Manager', and 'Condition List'. The main content area displays a report for wireless stations, filtered by 'By wireless station'. The report includes a search bar and a table of client connections.

Date time	MAC address	Alias	IP address	SSID	Band	Authentication	RSSI	Power save mode
2015-01-05 18:35:16	A088B4E4D508		192.168.0.100	WiFiManager50	5GHz	WPA2-Personal	84	OFF
2015-01-05 18:35:16	20A2E424BB95		192.168.0.120	WiFiManager50	5GHz	WPA2-Personal	73	OFF
2015-01-05 18:35:16	E0F5C602DB60		192.168.0.101	WiFiManager50	5GHz	WPA2-Personal	84	OFF
2015-01-05 18:35:18	001302696D71		192.168.0.109	WiFiManager50	5GHz	WPA2-Personal	92	OFF
2015-01-05 18:35:18	00EEBD7C0589		192.168.0.199	WiFiManager50	5GHz	WPA2-Personal	70	OFF
2015-01-05 18:36:16	20A2E424BB95		192.168.0.120	WiFiManager50	5GHz	WPA2-Personal	70	OFF
2015-01-05 18:36:16	A088B4E4D508		192.168.0.100	WiFiManager50	5GHz	WPA2-Personal	84	OFF
2015-01-05 18:36:16	E0F5C602DB60		192.168.0.101	WiFiManager50	5GHz	WPA2-Personal	76	OFF
2015-01-05 18:36:18	00EEBD7C0589		192.168.0.199	WiFiManager50	5GHz	WPA2-Personal	67	OFF
2015-01-05 18:36:18	001302696D71		192.168.0.109	WiFiManager50	5GHz	WPA2-Personal	92	OFF

10 total 1/1 Page

Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor

Report

Association


By Station Number

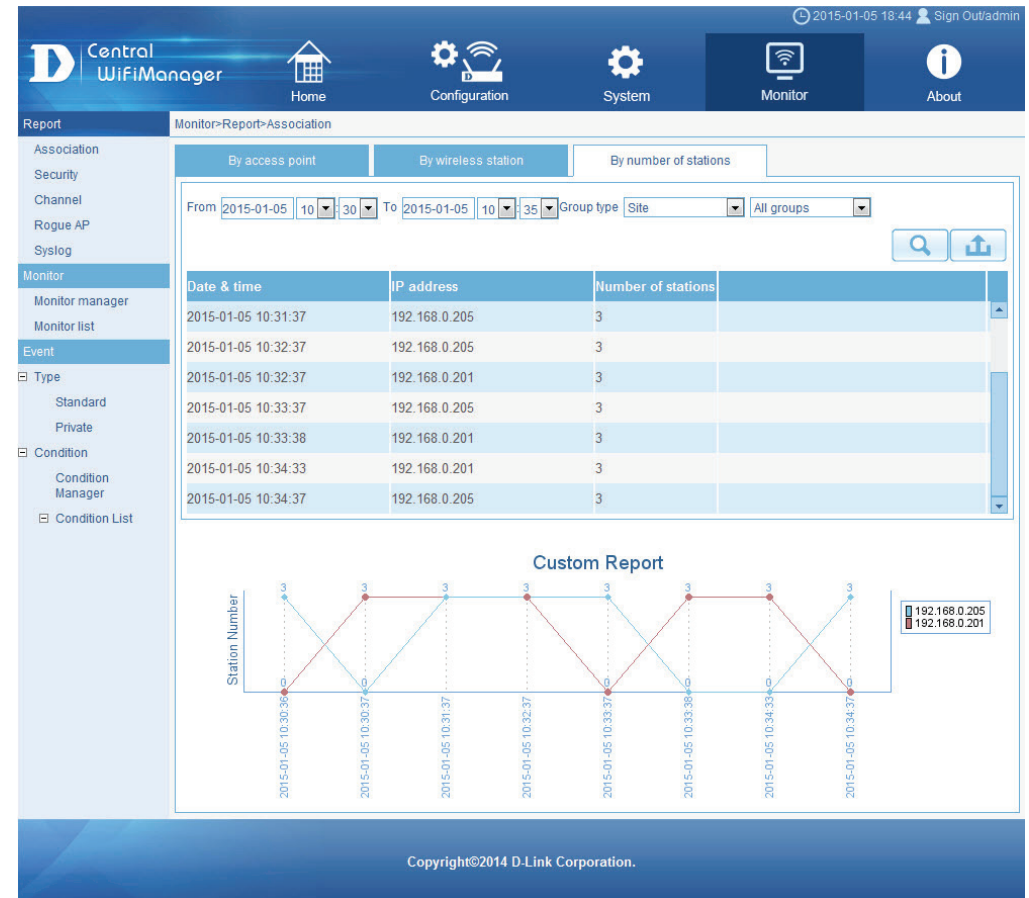
On this page a report was generated **By Station Number**. This report can be refined by selecting the date and time **From** and **To**, and then selecting the **Group Type** (Site), in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the  button to regenerate this report.

In the table a list of access points will be displayed, by station number, if they have active wireless client connections, connected to the access points, managed by this application. Information like **Date/Time**, **IP Address** and **Station's Number** is displayed for each station.

In the line graph, a graphical representation of the **Station Number** over time will be displayed per IP address.

Click the  button to export the contents displayed in this table and chart to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot displays the Central WiFiManager interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar contains a menu with 'Report' selected, and sub-items like 'Association', 'Security', 'Channel', 'Rogue AP', 'Syslog', 'Monitor', 'Monitor manager', 'Monitor list', 'Event', 'Type', 'Standard', 'Private', 'Condition', 'Condition Manager', and 'Condition List'.

The main content area shows the 'Monitor>Report>Association' page. It has three tabs: 'By access point', 'By wireless station', and 'By number of stations'. The 'By number of stations' tab is active. Below the tabs, there are filters for 'From' (2015-01-05 10:30:30), 'To' (2015-01-05 10:35:35), 'Group type' (Site), and 'All groups'. There are search and refresh buttons.

The table below shows the data for the report:

Date & time	IP address	Number of stations
2015-01-05 10:31:37	192.168.0.205	3
2015-01-05 10:32:37	192.168.0.205	3
2015-01-05 10:32:37	192.168.0.201	3
2015-01-05 10:33:37	192.168.0.205	3
2015-01-05 10:33:38	192.168.0.201	3
2015-01-05 10:34:33	192.168.0.201	3
2015-01-05 10:34:37	192.168.0.205	3

Below the table is a line graph titled 'Custom Report'. The Y-axis is 'Station Number' and the X-axis shows time intervals. Two lines represent the station numbers for IP addresses 192.168.0.205 (blue line) and 192.168.0.201 (red line). The graph shows the number of stations for each IP address over time, with values of 3 for both IP addresses at various time points.

Copyright©2014 D-Link Corporation.

CWM Configuration

Monitor


Report

Security


Chart

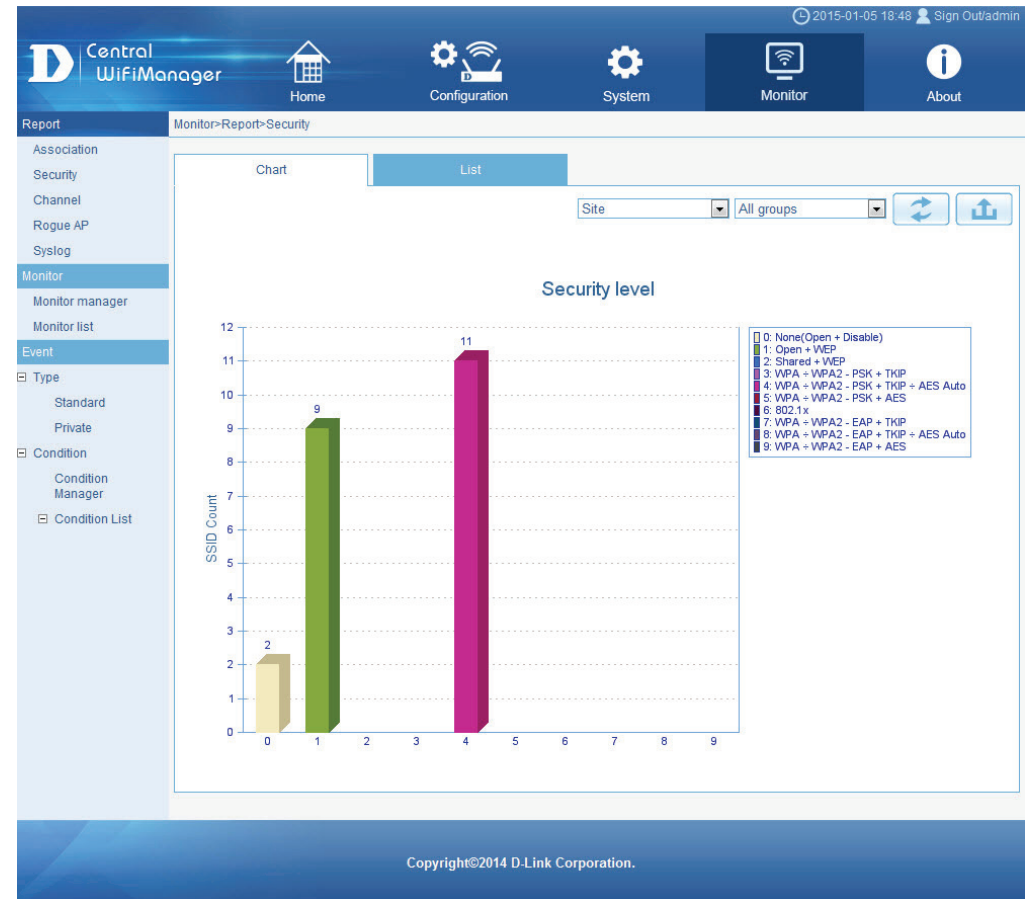
After clicking on **Monitor** in the top panel and **Security** in the left panel, the following page will be displayed. On this page we can view a report of the wireless security configurations of all the access points managed by this application. Security reports are displayed by **Chart** or by **List**.

On this page a **Chart** report was generated displaying all the available security levels on the access points managed by this application. This report can be refined by selecting the **Site**, in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the  button to regenerate this report.


This report counts the available amount of SSIDs hosted by the access points in the network and then evaluating which security level they are configured at and then presenting them graphically in this chart per security level.

Click the  button to export the contents displayed in this chart to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.




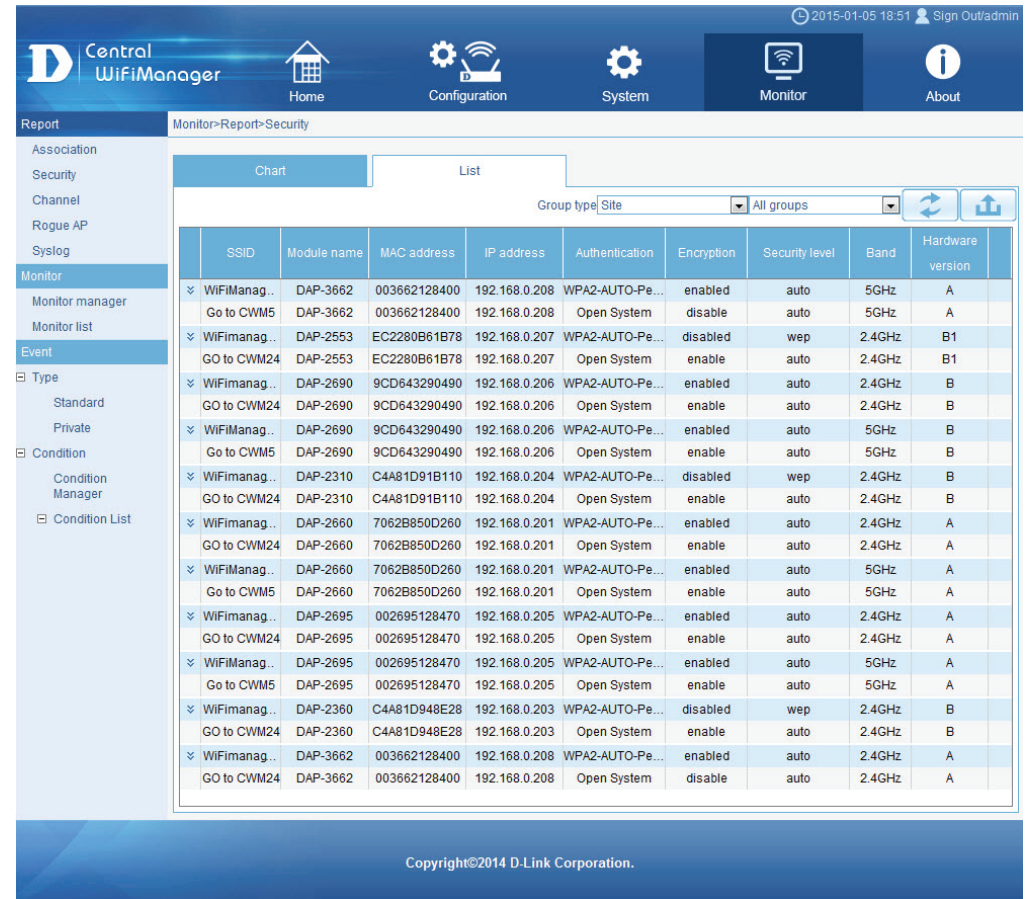
CWM Configuration Monitor Report Security **List**

On this page a **List** report was generated displaying all the SSIDs hosted by the access points managed by this application. This report can be refined by selecting the **Group Type** (Site), in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the  button to regenerate this report.

Information like **SSID, Module Name, MAC Address, IP Address, Authentication, Encryption, Security Level, Band** and **HW Version** is displayed for each SSID.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT, PDF** and **Excel**.



Report Monitor-Report>Security

Chart List

Group type: Site All groups


	SSID	Module name	MAC address	IP address	Authentication	Encryption	Security level	Band	Hardware version
WIFIManag...	DAP-3662	003662128400	192.168.0.208	WPA2-AUTO-Pe...	enabled	auto	5GHz	A	
Go to CWM5	DAP-3662	003662128400	192.168.0.208	Open System	disable	auto	5GHz	A	
WIFIManag...	DAP-2553	EC2280B61B78	192.168.0.207	WPA2-AUTO-Pe...	disabled	wep	2.4GHz	B1	
GO to CWM24	DAP-2553	EC2280B61B78	192.168.0.207	Open System	enable	auto	2.4GHz	B1	
WIFIManag...	DAP-2690	9CD643290490	192.168.0.206	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	B	
GO to CWM24	DAP-2690	9CD643290490	192.168.0.206	Open System	enable	auto	2.4GHz	B	
WIFIManag...	DAP-2690	9CD643290490	192.168.0.206	WPA2-AUTO-Pe...	enabled	auto	5GHz	B	
Go to CWM5	DAP-2690	9CD643290490	192.168.0.206	Open System	enable	auto	5GHz	B	
WIFIManag...	DAP-2310	C4A81D91B110	192.168.0.204	WPA2-AUTO-Pe...	disabled	wep	2.4GHz	B	
GO to CWM24	DAP-2310	C4A81D91B110	192.168.0.204	Open System	enable	auto	2.4GHz	B	
WIFIManag...	DAP-2660	7062B850D260	192.168.0.201	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	A	
GO to CWM24	DAP-2660	7062B850D260	192.168.0.201	Open System	enable	auto	2.4GHz	A	
WIFIManag...	DAP-2660	7062B850D260	192.168.0.201	WPA2-AUTO-Pe...	enabled	auto	5GHz	A	
Go to CWM5	DAP-2660	7062B850D260	192.168.0.201	Open System	enable	auto	5GHz	A	
WIFIManag...	DAP-2695	002695128470	192.168.0.205	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	A	
GO to CWM24	DAP-2695	002695128470	192.168.0.205	Open System	enable	auto	2.4GHz	A	
WIFIManag...	DAP-2695	002695128470	192.168.0.205	WPA2-AUTO-Pe...	enabled	auto	5GHz	A	
Go to CWM5	DAP-2695	002695128470	192.168.0.205	Open System	enable	auto	5GHz	A	
WIFIManag...	DAP-2360	C4A81D948E28	192.168.0.203	WPA2-AUTO-Pe...	disabled	wep	2.4GHz	B	
GO to CWM24	DAP-2360	C4A81D948E28	192.168.0.203	Open System	enable	auto	2.4GHz	B	
WIFIManag...	DAP-3662	003662128400	192.168.0.208	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	A	
GO to CWM24	DAP-3662	003662128400	192.168.0.208	Open System	disable	auto	2.4GHz	A	

Copyright©2014 D-Link Corporation.

CWM Configuration Monitor Report Channel


After clicking on **Monitor** in the top panel and **Channel** in the left panel, the following page will be displayed. On this page we can view a graphical chart report of the wireless channel usage per frequency band.

This report can be refined by selecting the **Group Type** (Site), in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the  button to regenerate this report.

In the first chart report, we can view the channel number count for the 2.4GHz wireless frequency band.

In the second chart report, we can view the channel number count for the 5GHz wireless frequency band.

Click the  button to export the contents displayed in these charts to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



CWM Configuration

Monitor


Report


Rogue AP

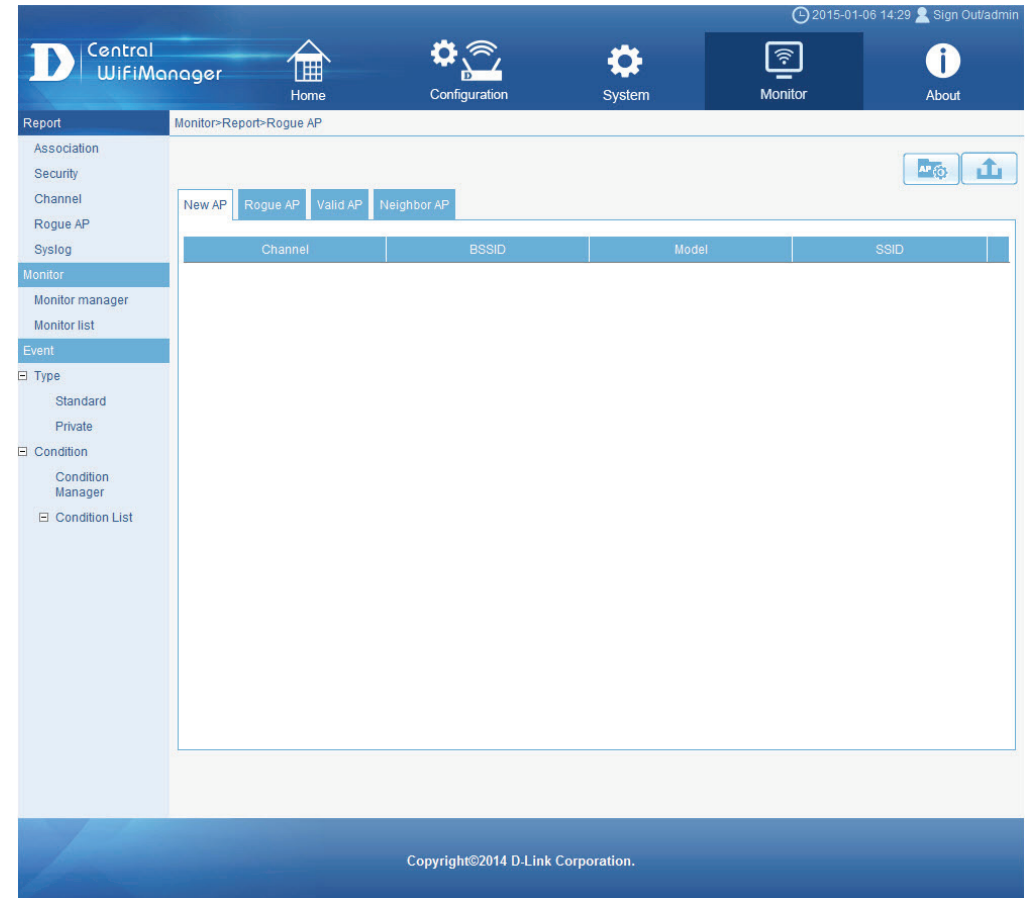
New AP

After clicking on **Monitor** in the top panel and **Rogue AP** in the left panel, the following page will be displayed. On this page we can view information about new, rogue, valid and neighboring access points. The purpose of this page is to scan for access points in the network and then to classify them into categories.

In the **New AP** tab, we can view a list of new access points in the environment. Access points displayed here have been detected by access points in our network and were classified as new access points.

Click the  button to scan for unclassified access points within the range of the access points connected to our network.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot displays the D-Link Central WifiManager interface. The top navigation bar includes Home, Configuration, System, Monitor, and About. The left sidebar shows the Report section expanded, with sub-items: Association, Security, Channel, Rogue AP, Syslog, Monitor, Monitor manager, Monitor list, Event, Type (Standard, Private), Condition (Condition Manager, Condition List). The main content area is titled "Monitor-Report-Rogue AP" and features a tabbed interface with "New AP", "Rogue AP", "Valid AP", and "Neighbor AP". The "New AP" tab is active, showing a table with columns: Channel, BSSID, Model, and SSID. The table is currently empty. There are two buttons in the top right of the table area: a scan button (AP icon with gear) and an export button (upload icon). The footer of the interface reads "Copyright©2014 D-Link Corporation." and the top right corner shows the date and time "2015-01-06 14:29" and "Sign Out/admin".


CWM Configuration

Monitor

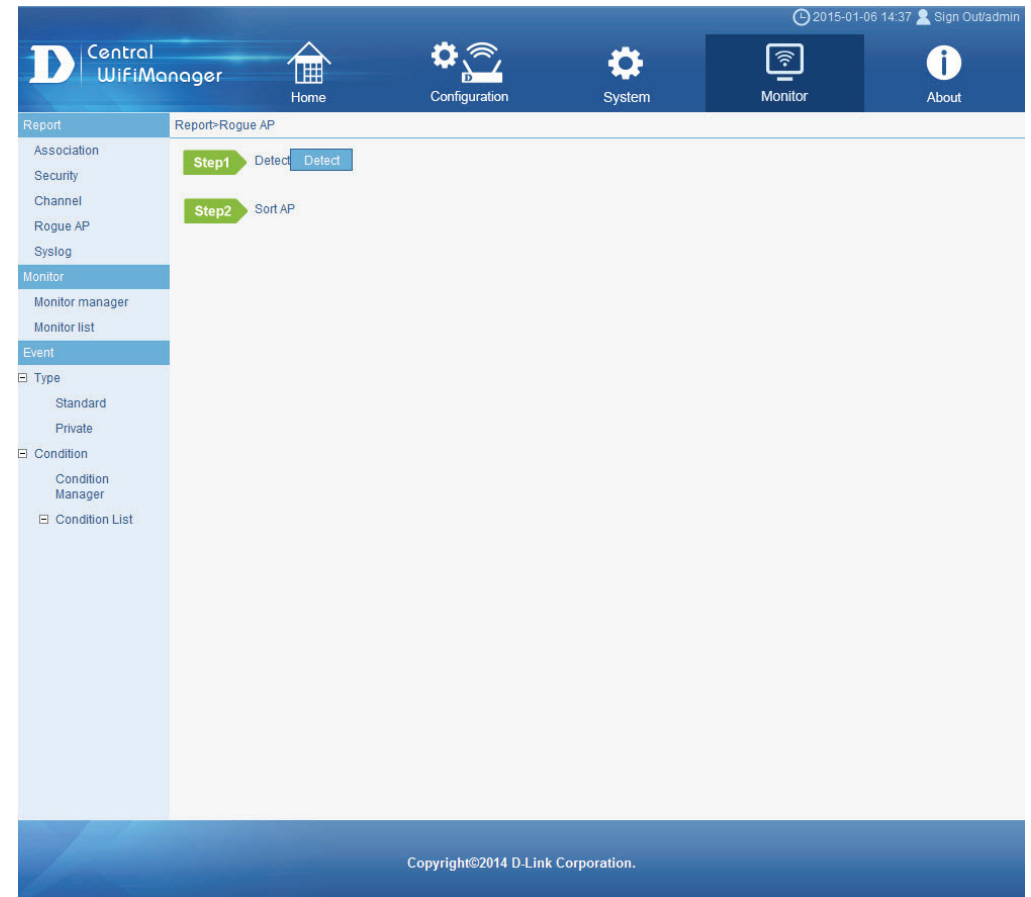
Report

Rogue AP

New AP

After clicking the  button, the following page will be available. On this page we can initiate a scan for unclassified access points within the wireless range of access points connected to our network.

Click the **Detect** button to initiate the scan.



The screenshot displays the Central WifiManager web interface. The top navigation bar includes the logo, "Home", "Configuration", "System", "Monitor", and "About" links. The main content area is titled "Report > Rogue AP" and shows a two-step process: "Step1 Detect" with a "Detect" button, and "Step2 Sort AP". The left sidebar contains a menu with categories: Report (Association, Security, Channel, Rogue AP, Syslog), Monitor (Monitor manager, Monitor list), and Event (Type: Standard, Private; Condition: Condition Manager, Condition List). The footer indicates "Copyright©2014 D-Link Corporation." and the top right shows the date "2015-01-06 14:37" and "Sign Out/admin".

CWM Configuration

Monitor

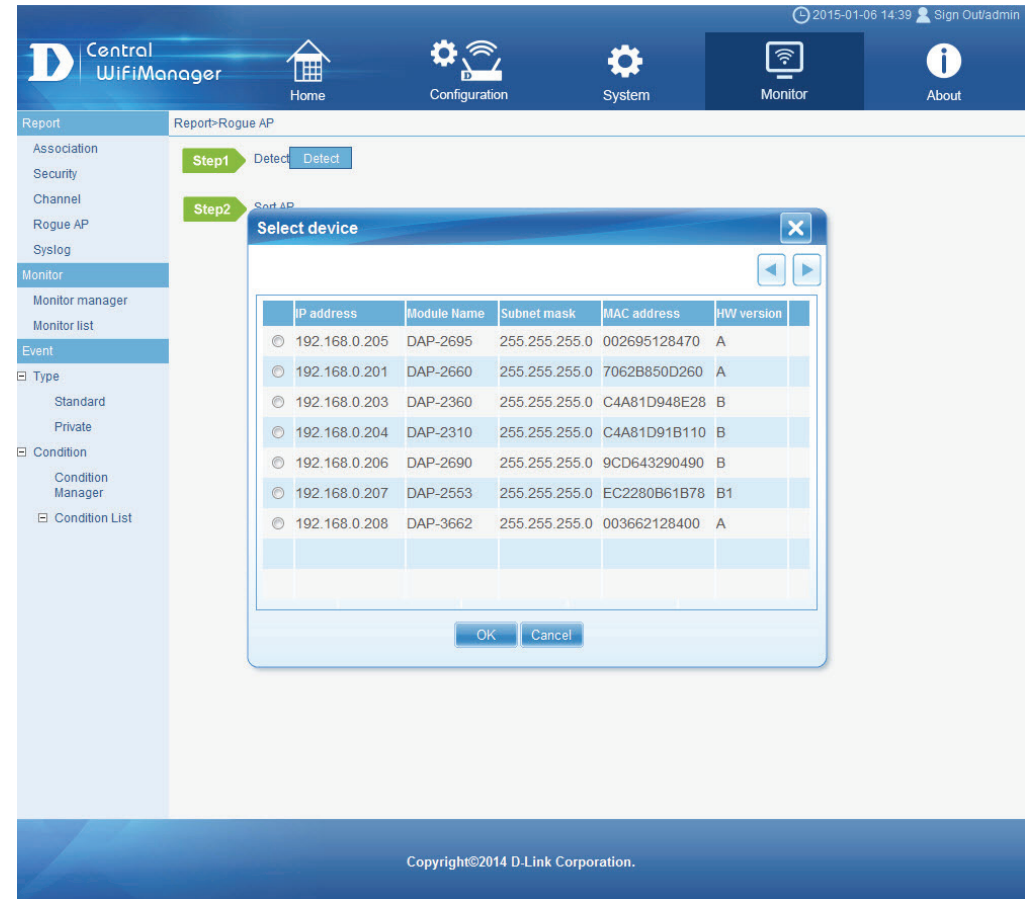
Report

Rogue AP

New AP

After clicking the **Detect** button, the following page will be available. On this page we can select an access point, in our network, that will be used for the scan.

After selecting an access point, click the **OK** button to start the scan.
Click the **Cancel** button to cancel the scan and return to the main page.



The screenshot shows the 'Report-Rogue AP' configuration page in the D-Link Central WifiManager interface. The page is divided into two main sections: 'Step1 Detect' and 'Step2 Select AP'. A 'Select device' dialog box is open, displaying a table of available access points for selection. The table has the following columns: IP address, Module Name, Subnet mask, MAC address, and HW version. The table contains 8 rows of data, with the first row selected.

	IP address	Module Name	Subnet mask	MAC address	HW version
<input checked="" type="radio"/>	192.168.0.205	DAP-2695	255.255.255.0	002695128470	A
<input type="radio"/>	192.168.0.201	DAP-2660	255.255.255.0	7062B850D260	A
<input type="radio"/>	192.168.0.203	DAP-2360	255.255.255.0	C4A81D948E28	B
<input type="radio"/>	192.168.0.204	DAP-2310	255.255.255.0	C4A81D91B110	B
<input type="radio"/>	192.168.0.206	DAP-2690	255.255.255.0	9CD643290490	B
<input type="radio"/>	192.168.0.207	DAP-2553	255.255.255.0	EC2280B61B78	B1
<input type="radio"/>	192.168.0.208	DAP-3662	255.255.255.0	003662128400	A

Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor

Report

Rogue AP

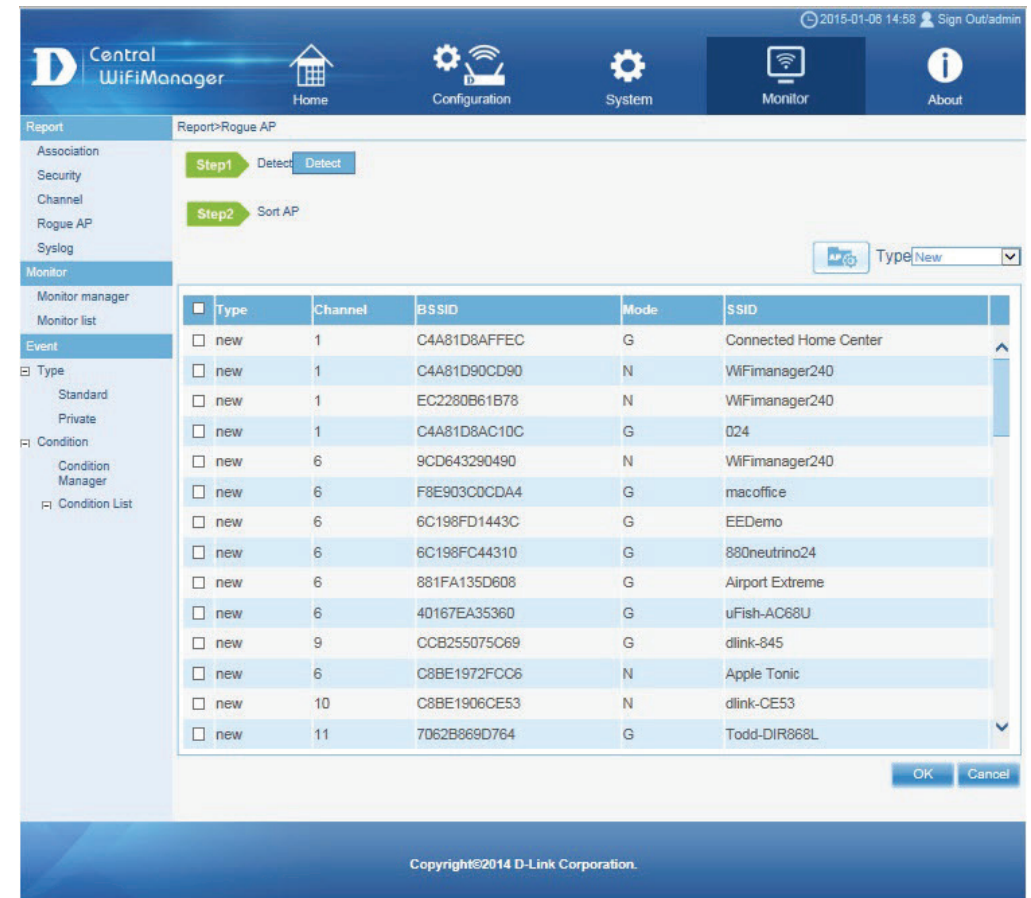
New AP

After clicking the **OK** button and after the scan was completed, this page will be available. On this page a list of unclassified access points within the wireless range of the previously select access point in our network will be displayed.

To classify access points in this list, select the check box next to the entry, click the  button and select the classification category from the list. Options to choose from are **New**, **Rogue**, **Neighborhood** and **Valid**.

To filter the display entries in the table to only display a certain category, select the **Type** option from the drop-down menu. Filter display options are **All**, **New**, **Rogue**, **Neighborhood** and **Valid**.

Click the **OK** button to classify the selected access points into the category selected. Click the **Cancel** button to cancel the process and return to the main page.



Central WifiManager

Home Configuration System Monitor About

Report>Rogue AP

Step1 Detect Detect

Step2 Sort AP

Type New

Type	Channel	BSSID	Mode	SSID
<input type="checkbox"/> new	1	C4A81D8AFFEC	G	Connected Home Center
<input type="checkbox"/> new	1	C4A81D90CD90	N	WiFiManager240
<input type="checkbox"/> new	1	EC2280B61B78	N	WiFiManager240
<input type="checkbox"/> new	1	C4A81D8AC10C	G	024
<input type="checkbox"/> new	6	9CD643290490	N	WiFiManager240
<input type="checkbox"/> new	6	F8E903C0CDA4	G	macoffice
<input type="checkbox"/> new	6	6C198FD1443C	G	EEDemo
<input type="checkbox"/> new	6	6C198FC44310	G	880neutrino24
<input type="checkbox"/> new	6	881FA135D608	G	Airport Extreme
<input type="checkbox"/> new	6	40167EA35360	G	uFish-AC68U
<input type="checkbox"/> new	9	CCB255075C69	G	dlink-845
<input type="checkbox"/> new	6	C8BE1972FCC6	N	Apple Tonic
<input type="checkbox"/> new	10	C8BE1906CE53	N	dlink-CE53
<input type="checkbox"/> new	11	7062B869D764	G	Todd-DIR868L

OK Cancel

Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor


Report

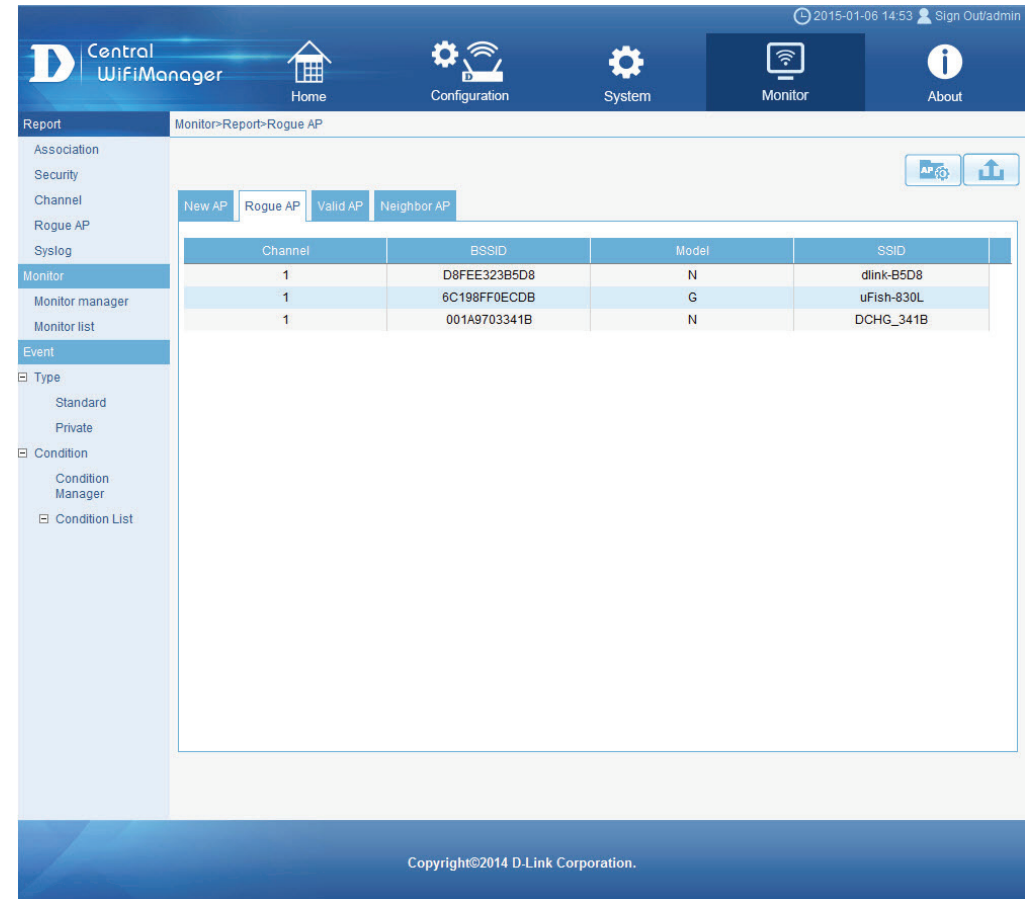
Rogue AP

Rogue AP

In the **Rogue AP** tab, we can view a list of access points in the environment that have been detected by access points in our network and were classified as rogue access points.

Click the  button to scan for unclassified access points within the range of the access points connected to our network.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot displays the D-Link Central WifiManager interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The 'Monitor' tab is active, and the 'Rogue AP' sub-tab is selected. The main content area shows a table of detected rogue access points.

Channel	BSSID	Model	SSID
1	D8FEE323B5D8	N	dlink-B5D8
1	6C198FF0ECDB	G	uFish-830L
1	001A9703341B	N	DCHG_341B

The interface also includes a sidebar with navigation options like 'Association', 'Security', 'Channel', 'Rogue AP', 'Syslog', 'Monitor', 'Monitor manager', and 'Monitor list'. The footer indicates 'Copyright©2014 D-Link Corporation.'

CWM Configuration


Monitor


Report

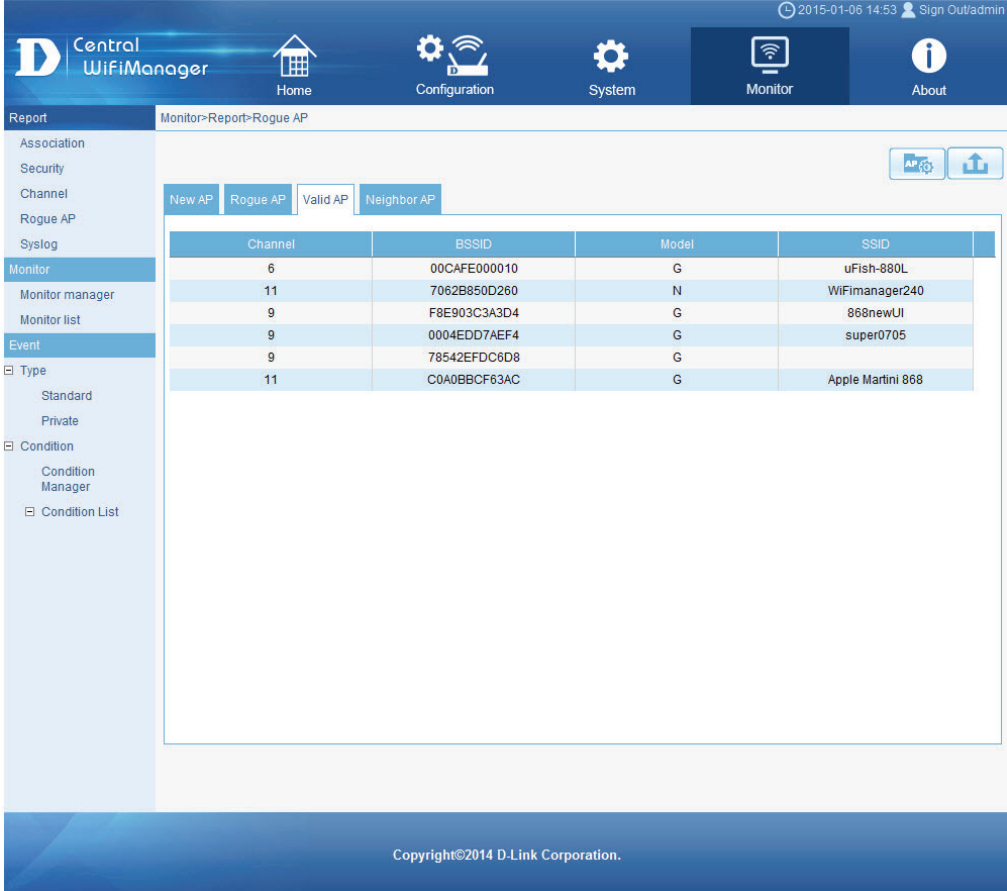
Rogue AP

Valid AP

In the **Valid AP** tab, we can view a list of access points in the environment that have been detected by access points in our network and were classified as valid access points.

Click the  button to scan for unclassified access points within the range of the access points connected to our network.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot shows the D-Link Central WifiManager interface. The top navigation bar includes the D-Link logo, the text 'Central WifiManager', and icons for Home, Configuration, System, Monitor, and About. The left sidebar contains a navigation menu with options: Report, Association, Security, Channel, Rogue AP, Syslog, Monitor (selected), Monitor manager, Monitor list, Event, Type (with sub-options Standard and Private), Condition (with sub-options Condition Manager and Condition List), and Condition List. The main content area is titled 'Monitor>Report>Rogue AP' and features a sub-menu with 'New AP', 'Rogue AP', 'Valid AP' (selected), and 'Neighbor AP'. Below the sub-menu is a table with the following data:

Channel	BSSID	Model	SSID
6	00CAFE000010	G	uFish-880L
11	7062B850D260	N	WiFiManager240
9	F8E903C3A3D4	G	868newUI
9	0004EDD7AEF4	G	super0705
9	78542EFD6D8	G	
11	C0A0BBCF63AC	G	Apple Martini 868

At the bottom of the interface, the copyright notice 'Copyright©2014 D-Link Corporation.' is visible.

CWM Configuration


Monitor


Report

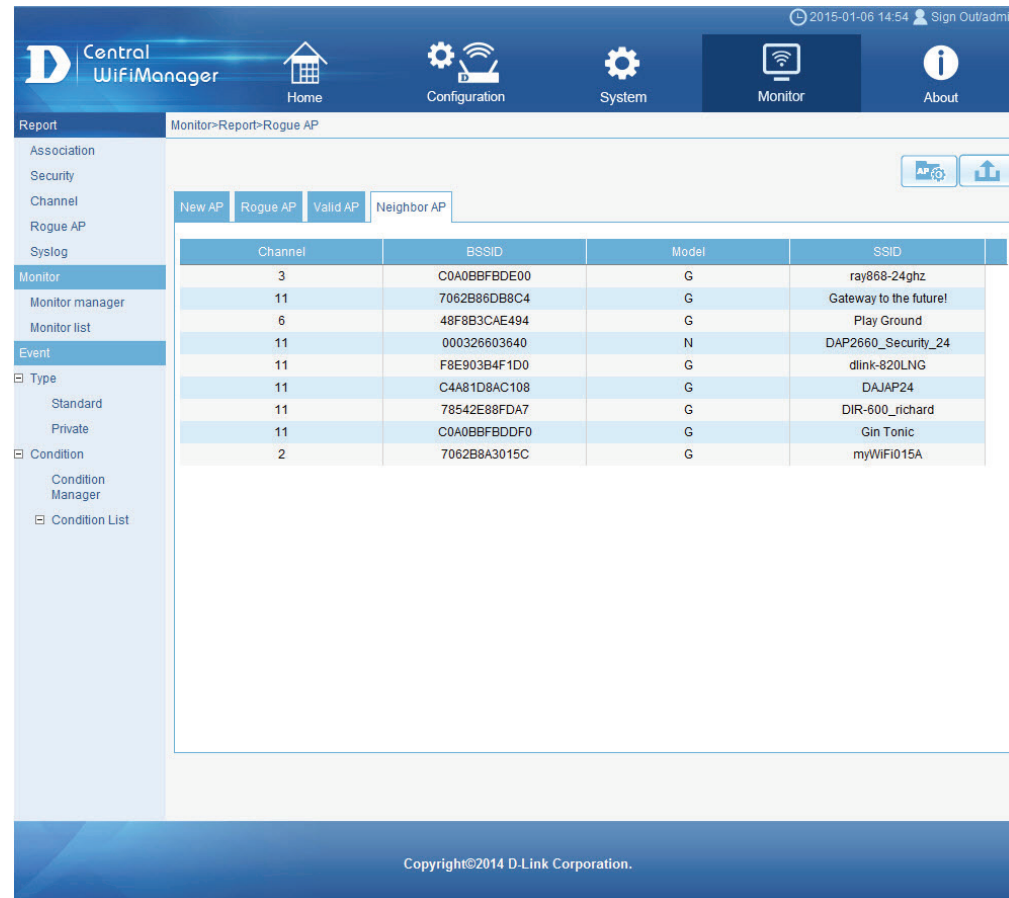
Rogue AP

Neighbor AP

In the **Neighbor AP** tab, we can view a list of access points in the environment that have been detected by access points in our network and were classified as neighbor access points.

Click the  button to scan for unclassified access points within the range of the access points connected to our network.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot displays the D-Link Central WifiManager interface. The top navigation bar includes Home, Configuration, System, Monitor, and About. The left sidebar shows a menu with options like Association, Security, Channel, Rogue AP, Syslog, Monitor, Monitor manager, Monitor list, Event, Type (Standard, Private), Condition, Condition Manager, and Condition List. The main content area is titled 'Monitor-Report-Rogue AP' and features a 'Neighbor AP' tab. Below the tabs is a table with the following data:

Channel	BSSID	Model	SSID
3	C0A0BBFBDE00	G	ray868-24ghz
11	7062B86DB8C4	G	Gateway to the future!
6	48F8B3CAE494	G	Play Ground
11	000326603640	N	DAP2660_Security_24
11	F8E903B4F1D0	G	dlink-820LNG
11	C4A81D8AC108	G	DAJAP24
11	78542E88FDA7	G	DIR-600_richard
11	C0A0BBFBDDF0	G	Gin Tonic
2	7062B8A3015C	G	myWIFI015A

Copyright©2014 D-Link Corporation.


CWM Configuration

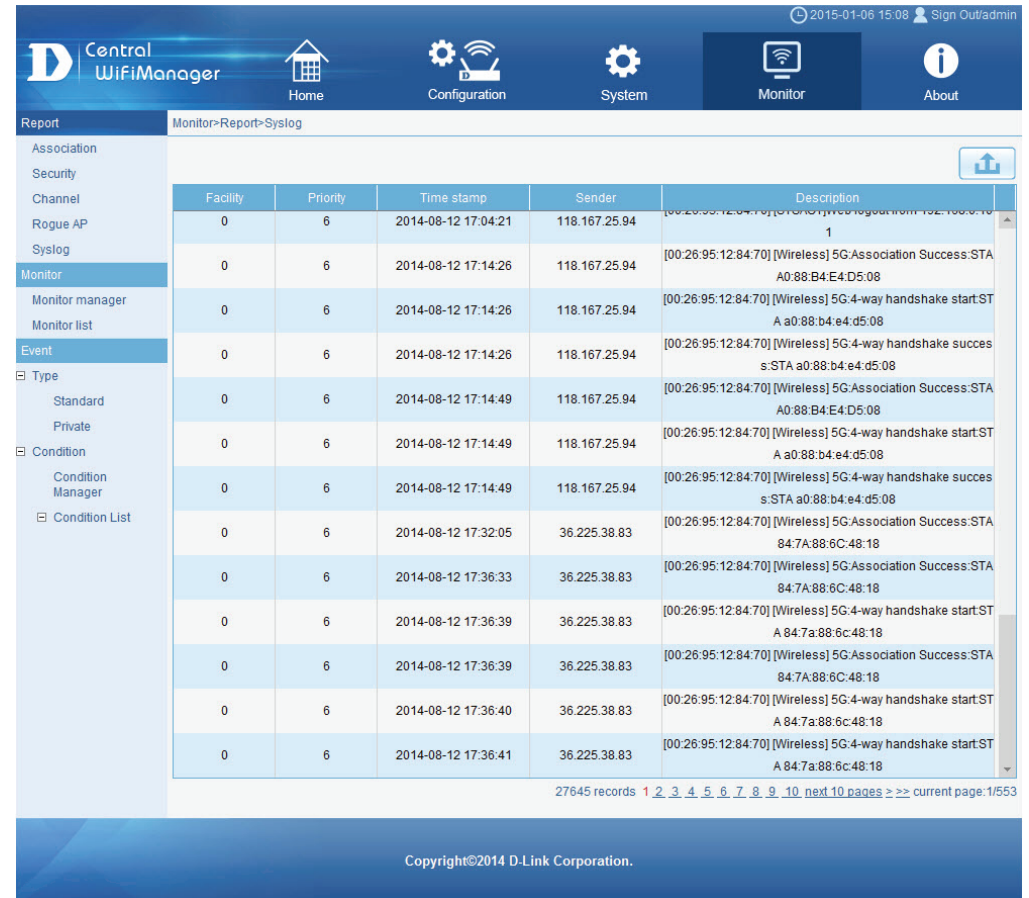
Monitor

Report

SysLog

After clicking on **Monitor** in the top panel and **SysLog** in the left panel, the following page will be displayed. On this page we can view system log entries generated by events that occurred on the network and events that occurred on the Central WifiManager Server application.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



The screenshot shows the Central WifiManager interface with the 'Monitor' tab selected. The left sidebar shows a tree view with 'Event' expanded to 'Syslog'. The main area displays a table of log entries. The table has the following columns: Facility, Priority, Time stamp, Sender, and Description. The entries show various wireless events such as '5G:Association Success' and '5G:4-way handshake start' for different MAC addresses. At the bottom of the table, it indicates '27645 records' and provides pagination options. An export icon is visible in the top right corner of the table area.

Facility	Priority	Time stamp	Sender	Description
0	6	2014-08-12 17:04:21	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G:Association Success:STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:26	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake start:STA A a0:88:b4:e4:d5:08
0	6	2014-08-12 17:14:26	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake success:STA a0:88:b4:e4:d5:08
0	6	2014-08-12 17:14:49	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G:Association Success:STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:49	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake start:STA A a0:88:b4:e4:d5:08
0	6	2014-08-12 17:14:49	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake success:STA a0:88:b4:e4:d5:08
0	6	2014-08-12 17:32:05	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G:Association Success:STA 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:33	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G:Association Success:STA 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:39	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake start:STA A 84:7a:88:6c:48:18
0	6	2014-08-12 17:36:39	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G:Association Success:STA 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:40	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake start:STA A 84:7a:88:6c:48:18
0	6	2014-08-12 17:36:41	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G:4-way handshake start:STA A 84:7a:88:6c:48:18

27645 records 1 2 3 4 5 6 7 8 9 10 next 10 pages >>> current page: 1/553

Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor


Monitor


Monitor Manager

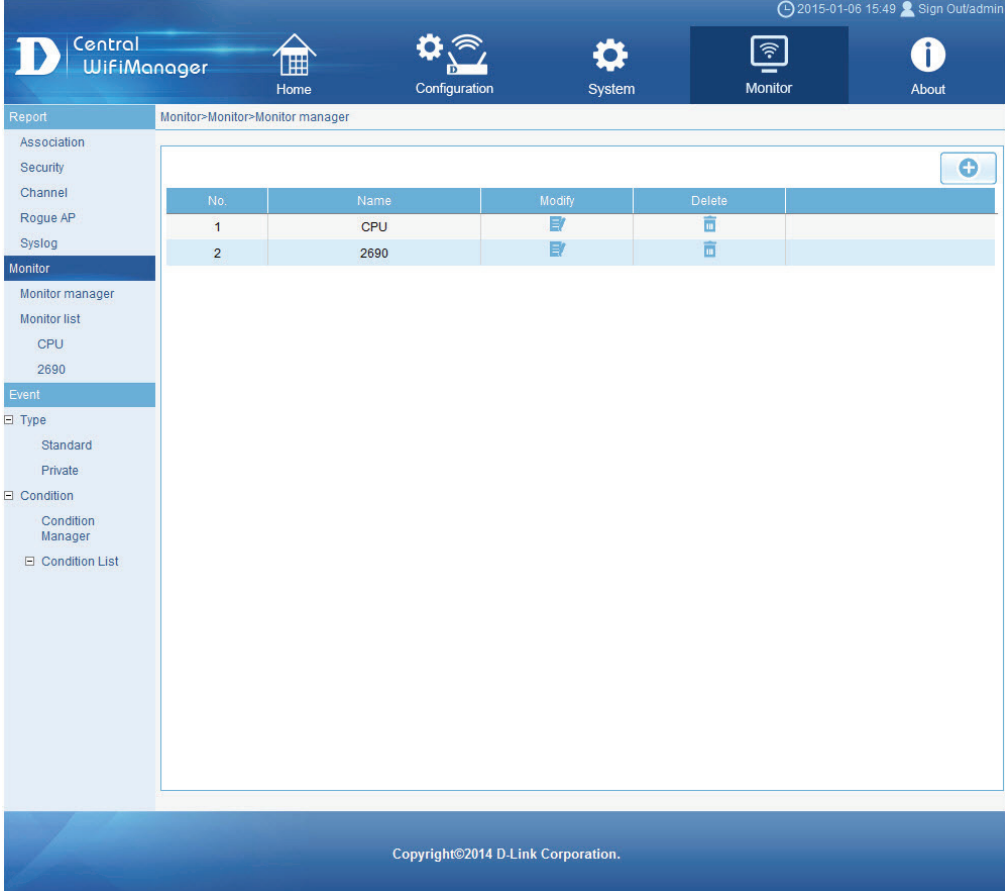
After clicking on **Monitor** in the top panel and **Monitor Manager** in the left panel, the following page will be displayed. On this page we can view, create and configure monitoring watchdog entries to specifically monitor certain events that take place on certain devices.

On this page, a list of monitor manager watchdog entries are displayed.





Click the  button to create a new monitor manager entry.

Click the  icon to modify an existing monitor manager entry.

Click the  icon to delete an existing monitor manager entry.



Report Monitor>Monitor>Monitor manager

No.	Name	Modify	Delete
1	CPU		
2	2690		

Copyright©2014 D-Link Corporation.


CWM Configuration

Monitor

Monitor

Monitor Manager

Create Profile

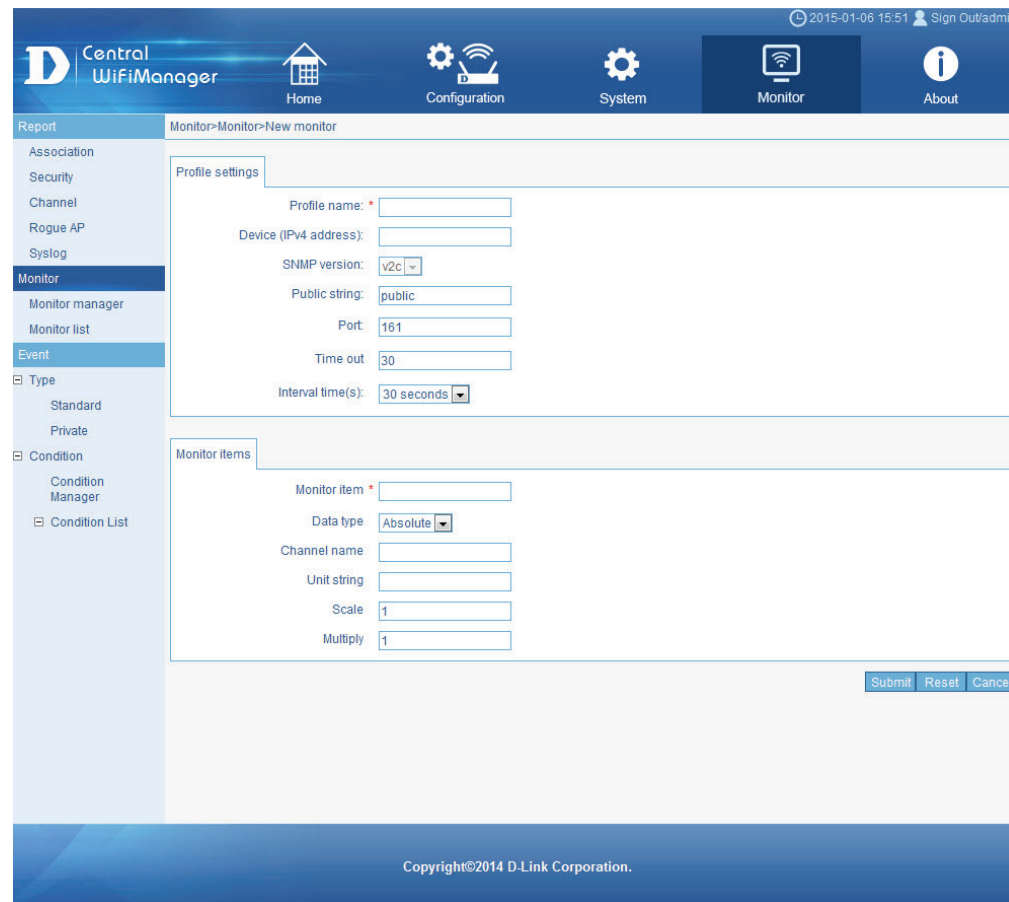
After clicking on the add  icon, the following page will be available. On this page we can create or configure a monitor manager watchdog entry.

In the **Profile Settings** section, the following parameters can be configured:

Parameter	Description
Profile Name	Enter the profile name here. This name will be used to identify the entry in the list.
Device (IPv4 Address)	Click in the text box to view a list of access points associated with our network. Select an entry and click OK to add it to this field.
SNMP Version	This field will display the SNMP version that will be used for this entry. By default, the version is SNMPv2c .
Public String	Enter the public SNMP string name here. By default, this string is public .
Port	Enter the port number that the SNMP agent will use to receive request messages. By default, this value is UDP port number 161.
Timeout	Enter the message timeout value here. By default, this value is 30.
Interval Time(s)	Enter the interval time value here. By default, this value is 30 seconds.

In the **Monitor Items** section, the following parameters can be configured:

Parameter	Description
Monitor Item	Click in this text box to view a list of monitor items available for selection. Select a monitor item from the list. Options available for selection are TransmittedByte-2.4G , ReceivedByte-2.4G , TransmittedByte-5G , ReceivedByte-5G , and CPUUtilization .
Data Type	Select the data type here. Options to choose from are Absolute and Relative .
Channel Name	Enter the channel name here.
Unit String	Enter the unit string here.
Scale	Enter the scale value here.
Multiply	Enter the multiply value here.



The screenshot shows the 'Central WifiManager' web interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar lists various configuration sections: Report, Association, Security, Channel, Rogue AP, Syslog, Monitor (selected), Monitor manager, Monitor list, Event, Type (Standard, Private), Condition, Condition Manager, and Condition List. The main content area is titled 'Monitor>Monitor>New monitor' and is divided into two sections: 'Profile settings' and 'Monitor items'. The 'Profile settings' section contains fields for Profile name, Device (IPv4 address), SNMP version (set to v2c), Public string (set to public), Port (set to 161), Time out (set to 30), and Interval time(s) (set to 30 seconds). The 'Monitor items' section contains fields for Monitor item, Data type (set to Absolute), Channel name, Unit string, Scale (set to 1), and Multiply (set to 1). At the bottom right of the form are buttons for 'Submit', 'Reset', and 'Cancel'. The footer of the page reads 'Copyright©2014 D-Link Corporation.'

Click the **Submit** button to accept the changes made.
 Click the **Reset** button to clear out the information entered in the fields above.
 Click the **Cancel** button to discard the changes made and return to the main page.

CWM Configuration


Monitor


Monitor


Monitor List

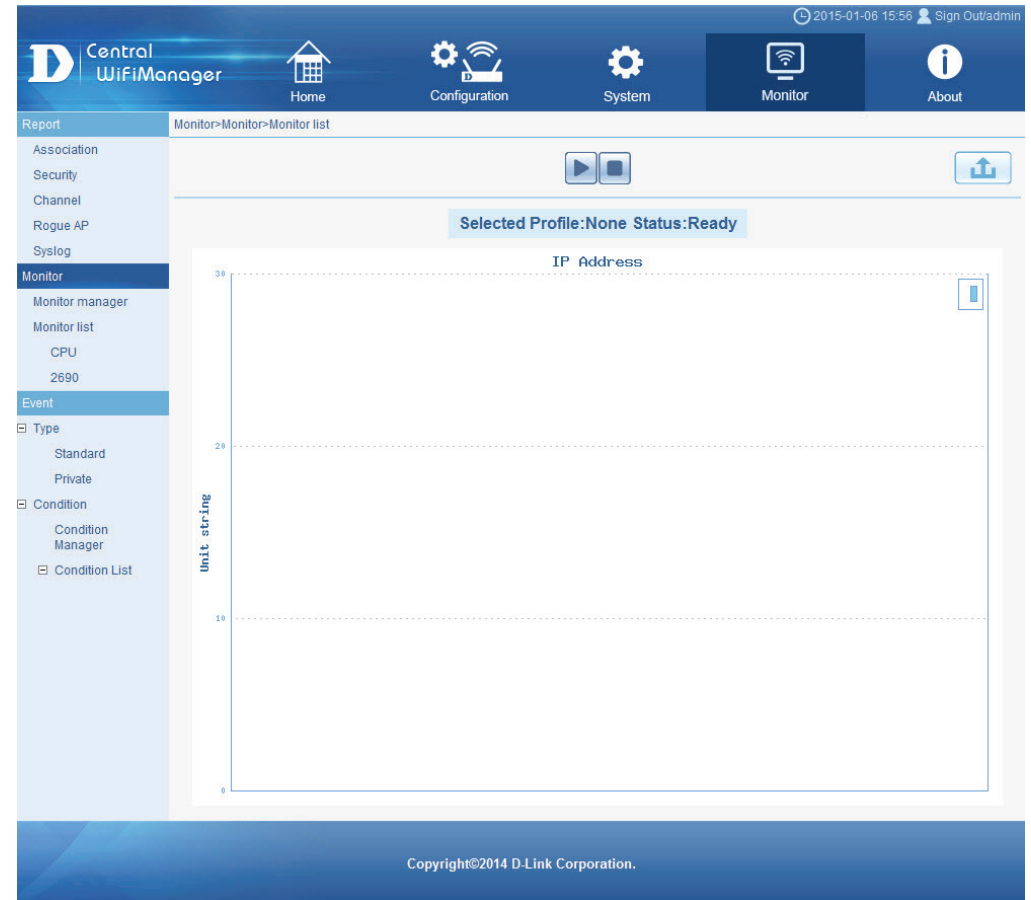
After clicking on **Monitor** in the top panel and **Monitor List** in the left panel, the following page will be displayed. On this page we can view a graphical chart of the monitor manager watchdog events create on the previous page. The list of created events will be displayed under the monitor list option in the left panel.

In this example, we created a monitor manager event called **Access-Point-1**.

Click the  button to run the monitor event.

Click the  button to stop the monitor event.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file format; **PNG**.



Central WifiManager

Home Configuration System Monitor About

Report Monitor-Monitor-Monitor list

Association Security Channel Rogue AP Syslog Monitor Monitor manager Monitor list CPU 2690 Event Type Standard Private Condition Condition Manager Condition List

Selected Profile:None Status:Ready

IP Address

Unit string


Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor


Monitor

Monitor List

After clicking the  button, the monitor manager event will run and real-time updates will be displayed in the chart.

In this chart, we monitor the transmitted data of the 2.4GHz frequency band of the access point with the IP address of 192.168.70.50 at 30 second intervals using SNMPv2c and the public string.

Click the  button to export this chart. This chart will be exported as an image file with the file format of **PNG**.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file format; **PNG**.




CWM Configuration Monitor Event Type Standard


After clicking on **Monitor** in the top panel and **Event > Type > Standard** in the left panel, the following page will be displayed. On this page we can view standard event type messages generated based on the **Event & Notice Settings** configuration. A standard event is an event that can occur on all devices managed by the Central WifiManager Server application.

In the table, we can choose to display events based on the filtering criteria selected or we can choose to display all events generated.


To filter the events displayed in the table, the following parameters can be configured:

Parameter	Description
Date	Select the starting date by clicking in the first text box available and select the starting date from the option available. Do the same for the ending date selection in the second text box.
Event Level	Select the event level from the drop-down list provided. Options to choose from are all , critic , error , warning , and notice .
Node IP	Enter the node's IP address here.
Keyword	To display only entries that contain a certain keyword, enter that keyword in this text box.


Click the  button to display only the entries based on the criteria entered.

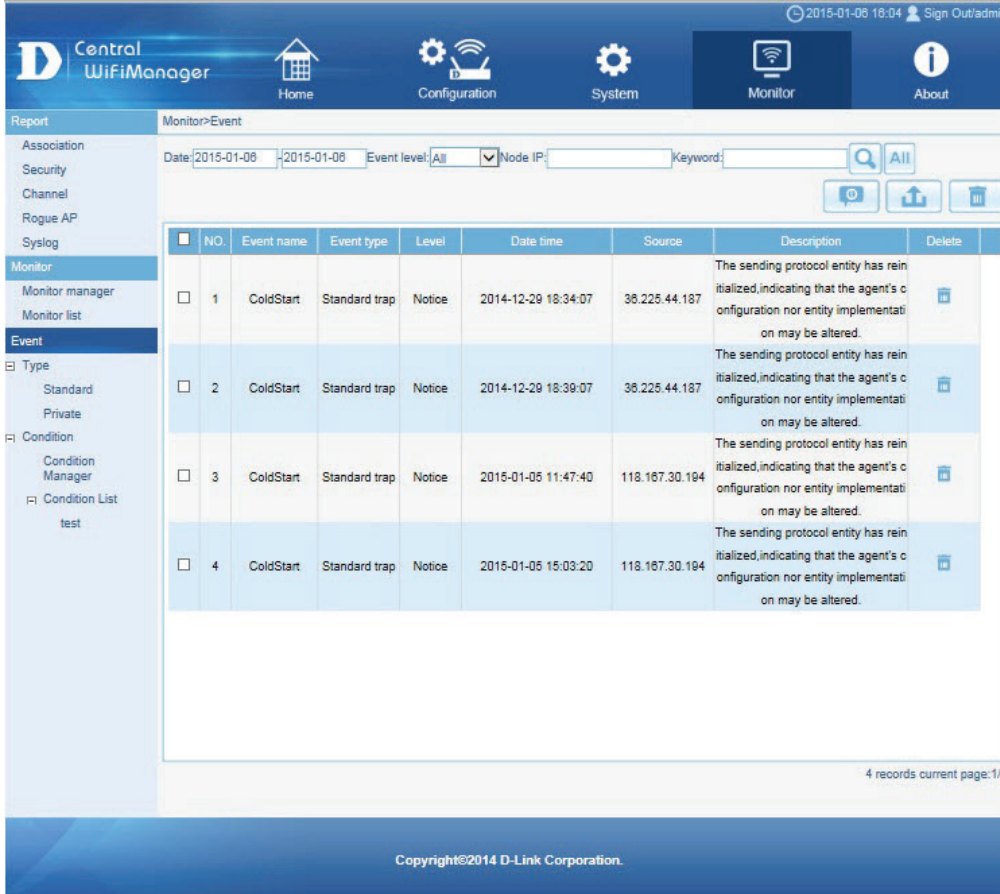
Click the  button to display all standard events that have taken place.





Click the  button to create a new standard event and notice.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.


Click the big  button to remove all entries from the event table.

Click the small  button next to a specific entry to remove only that entry from the event table.



NO.	Event name	Event type	Level	Date time	Source	Description	Delete
1	ColdStart	Standard trap	Notice	2014-12-29 18:34:07	36.225.44.187	The sending protocol entity has reinitialized, indicating that the agent's configuration nor entity implementation may be altered.	
2	ColdStart	Standard trap	Notice	2014-12-29 18:39:07	36.225.44.187	The sending protocol entity has reinitialized, indicating that the agent's configuration nor entity implementation may be altered.	
3	ColdStart	Standard trap	Notice	2015-01-05 11:47:40	118.167.30.194	The sending protocol entity has reinitialized, indicating that the agent's configuration nor entity implementation may be altered.	
4	ColdStart	Standard trap	Notice	2015-01-05 15:03:20	118.167.30.194	The sending protocol entity has reinitialized, indicating that the agent's configuration nor entity implementation may be altered.	

CWM Configuration Monitor Event Type Standard **Event**

After clicking the  button, the following page will be available. On this page, we can configure the standard SNMP event and notice settings that will be used to display messages on the **Standard** page, when that type of event has occurred on the network. For a complete list of standard traps that are supported by this application, refer to “**Appendix B - Standard & Private Trap List**” on page <OV>.

In the **Event** tab, the following parameters can be configured:

Parameter	Description
Event	To modify an existing standard trap, select it in this section. After selecting an existing trap, its parameters will automatically be entered in the Event Settings section for modification. To create a new trap, do not select any event in this section.
SNMP Version	Select the SNMP version that will be used for this trap here. Options to choose from are SNMPv1 and SNMPv2c . When modifying an existing trap, this field cannot be changed.
Event Name	Enter the event's name here. This name will be used to identify the event in the table mentioned before.
Generic TRAP Types	Select the generic trap that will be used for this new trap here. Options to choose from are Coldstart(0) , WarmStart(1) , LinkDown(2) , LinkUp(3) , AuthenticationFailure(4) , EgpNeighborLoss(5) , and EnterpriseSpecific(6) . When modifying an existing trap, this field cannot be changed.
Status	Select to Enable or Disable this specific trap here.
OID	Enter the Object Identifier (OID) number for this trap here. When modifying an existing trap, this field cannot be changed.
Description	Enter the trap's description here.
Level	Select the level for this trap here. Options to choose from are Critical , Error , Warning , and Notice .

Click the **New** button create a new trap event.

Click the **Save** button to accept the changes made.

Click the **Delete** button to delete the selected trap.

Click the **OK** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

CWM Configuration

Monitor

Event

Type

Standard

Notice

In the **Notice** tab, we can enable the notification feature when a standard trap event was generated for a specific warning level.

The following parameters can be configured:

Parameter	Description
Warning Level	Select the warning level here. Options to choose from are Critical, Error, Warning, and Notice.
Send E-Mail	After the warning level was selected, select this option to enable the email notification feature for the selected warning level.
Recipient	Enter the recipient's email address here.
Sender	Enter the sender's email address here.
Subject	Enter the subject for the message here.
Message Type	Select the message type here. Options to choose from are Event Level, Event Date/Time, Device Target, and Event Notice.
Remark	Enter the remark for this message here.

Click the **Apply** button to accept the changes made.

Click the **OK** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

The screenshot displays the 'Central WifiManager' web interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar shows a tree view with 'Event' selected. The main content area is titled 'Report-Event-Event & notice settings' and has two tabs: 'Event' and 'Notice'. The 'Notice' tab is active, showing a 'Warning level' dropdown menu with options: Critical, Error, Warning, and Notice. To the right, the 'E-mail notification settings' section includes a 'Send e-mail' checkbox, fields for 'Recipient', 'Sender', and 'Subject', and a 'Message type' section with checkboxes for 'Event level', 'Event date & time', 'Device target', and 'Event notice'. A 'Remark' text area is also present. At the bottom right of the settings area is an 'Apply' button. At the very bottom of the page are 'OK' and 'Cancel' buttons. The footer indicates 'Copyright©2014 D-Link Corporation.'


CWM Configuration Monitor Event Type Private

After clicking on **Monitor** in the top panel and **Event > Type > Private** in the left panel, the following page will be displayed. On this page we can view private event type messages generated based on the **Event & Notice Settings** configuration. A private event is an event that can only occur on specific devices that are managed by the Central WifiManager Server application. These events are product specific. For a complete list of private traps that are supported by this application, refer to “**Appendix B - Standard & Private Trap List**” on page <OV>.

In the table, we can choose to display events based on the filtering criteria selected or we can choose to display all events generated.


To filter the events displayed in the table, the following parameters can be configured:

Parameter	Description
Date	Select the starting date by clicking in the first text box available and select the starting date from the option available. Do the same for the ending date selection in the second text box.
Event Level	Select the event level from the drop-down list provided. Options to choose from are all , critic , error , warning , and notice .
Node IP	Enter the node's IP address here.
Keyword	To display only entries that contain a certain keyword, enter that keyword in this text box.


Click the  button to display only the entries based on the criteria entered.

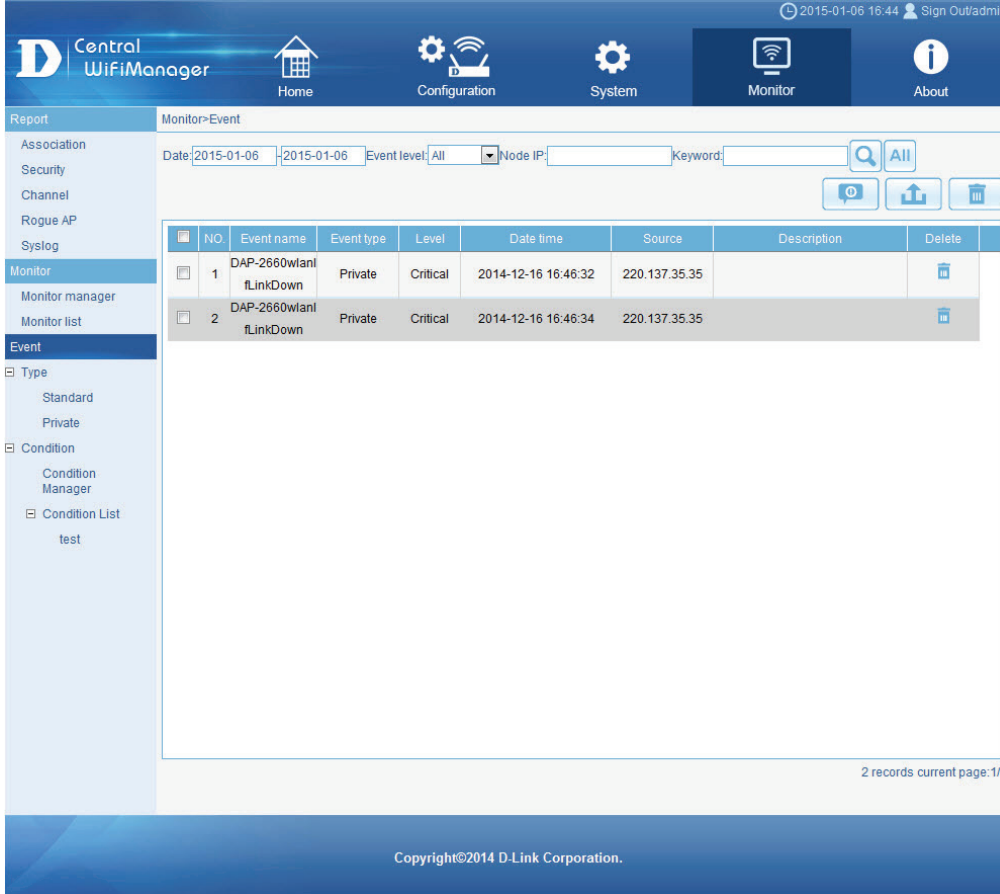
Click the  button to display all private events that have taken place.

Click the  button to create a new private event and notice.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

Click the big  button to remove all entries from the event table.

Click the small  button next to a specific entry to remove only that entry from the event table.





Central WifiManager

Home Configuration System Monitor About

Report Monitor>Event

Date: 2015-01-06 - 2015-01-06 Event level: All Node IP: Keyword:

NO	Event name	Event type	Level	Date time	Source	Description	Delete
1	DAP-2660wlan1 fLinkDown	Private	Critical	2014-12-16 16:46:32	220.137.35.35		
2	DAP-2660wlan1 fLinkDown	Private	Critical	2014-12-16 16:46:34	220.137.35.35		

2 records current page: 1/1

Copyright©2014 D-Link Corporation.

CWM Configuration


Monitor

Event

Type

Private

Event

After clicking the  button, the following page will be available. On this page, we can configure the private SNMP event and notice settings that will be used to display messages on the **Private** page, when that type of event has occurred on the network.

In the **Event** tab, the following parameters can be configured:

Parameter	Description
Event	To modify an existing private trap, select it in this section. After selecting an existing trap, its parameters will automatically be entered in the Event Settings section for modification. To create a new trap, do not select any event in this section.
SNMP Version	Select the SNMP version that will be used for this trap here. Options to choose from are SNMPv1 and SNMPv2c . When modifying an existing trap, this field cannot be changed.
Event Name	Enter the event's name here. This name will be used to identify the event in the table mentioned before.
Generic TRAP Types	Select the generic trap that will be used for this new trap here. Options to choose from are Coldstart(0) , WarmStart(1) , LinkDown(2) , LinkUp(3) , AuthenticationFailure(4) , EgpNeighborLoss(5) , and EnterpriseSpecific(6) . When modifying an existing trap, this field cannot be changed.
Status	Select to Enable or Disable this specific trap here.
OID	Enter the Object Identifier (OID) number for this trap here. When modifying an existing trap, this field cannot be changed.
Description	Enter the trap's description here.
Level	Select the level for this trap here. Options to choose from are Critical , Error , Warning , and Notice .

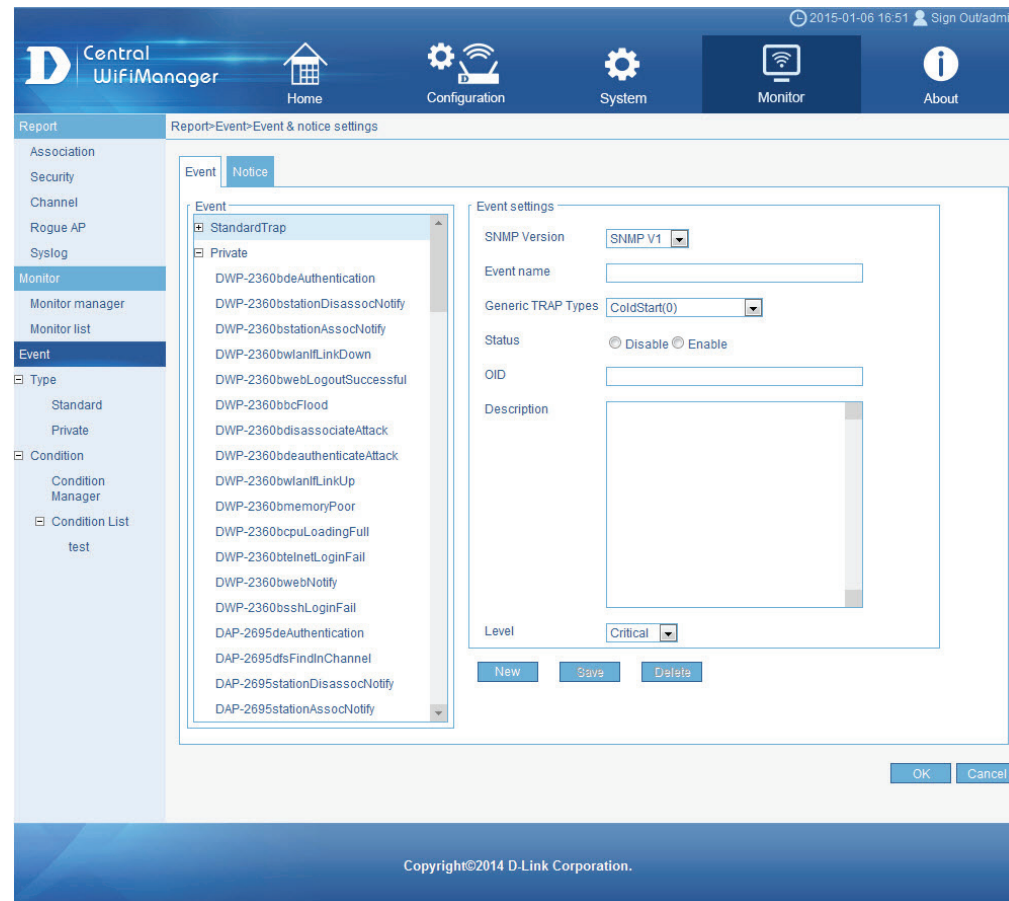
Click the **New** button create a new trap event.

Click the **Save** button to accept the changes made.

Click the **Delete** button to delete the selected trap.

Click the **OK** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



The screenshot displays the Central WifiManager configuration interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar shows a tree view with 'Event' selected under 'Monitor'. The main content area is titled 'Report-Event-Event & notice settings' and contains two tabs: 'Event' and 'Notice'. The 'Event' tab is active, showing a list of event types under 'StandardTrap' and 'Private'. The 'Private' section is expanded, listing various event types such as 'DWP-2360bdeAuthentication', 'DWP-2360bstationDisassocNotify', 'DWP-2360bstationAssocNotify', 'DWP-2360bwlanflLinkDown', 'DWP-2360bwebLogoutSuccessful', 'DWP-2360bbcFlood', 'DWP-2360bdisassociateAttack', 'DWP-2360bdeauthenticateAttack', 'DWP-2360bwlanflLinkUp', 'DWP-2360bmemoryPoor', 'DWP-2360bcpuLoadingFull', 'DWP-2360bteinetLoginFail', 'DWP-2360bwebNotify', 'DWP-2360bsshLoginFail', 'DAP-2695deAuthentication', 'DAP-2695dfsFindInChannel', 'DAP-2695stationDisassocNotify', and 'DAP-2695stationAssocNotify'. The 'Event settings' panel on the right includes fields for 'SNMP Version' (set to 'SNMP V1'), 'Event name', 'Generic TRAP Types' (set to 'ColdStart(0)'), 'Status' (radio buttons for 'Disable' and 'Enable'), 'OID', and 'Description'. A 'Level' dropdown is set to 'Critical'. At the bottom of the settings panel are 'New', 'Save', and 'Delete' buttons. The bottom of the interface shows 'OK' and 'Cancel' buttons and a copyright notice: 'Copyright©2014 D-Link Corporation.'

CWM Configuration

Monitor

Event

Type

Private

Notice

In the **Notice** tab, we can enable the notification feature when a private trap event was generated for a specific warning level.

The following parameters can be configured:

Parameter	Description
Warning Level	Select the warning level here. Options to choose from are Critical, Error, Warning, and Notice.
Send E-Mail	After the warning level was selected, select this option to enable the email notification feature for the selected warning level.
Recipient	Enter the recipient's email address here.
Sender	Enter the sender's email address here.
Subject	Enter the subject for the message here.
Message Type	Select the message type here. Options to choose from are Event Level, Event Date/Time, Device Target, and Event Notice.
Remark	Enter the remark for this message here.

Click the **Apply** button to accept the changes made.

Click the **OK** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

The screenshot displays the Central WifiManager web interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar shows a tree view with 'Event' selected under the 'Monitor' section. The main content area is titled 'Report-Event-Event & notice settings' and has two tabs: 'Event' and 'Notice'. The 'Notice' tab is active, showing a 'Warning level' dropdown menu with options: Critical, Error, Warning, and Notice. To the right, the 'E-mail notification settings' section includes a 'Send e-mail' checkbox, input fields for 'Recipient', 'Sender', and 'Subject', and a 'Message type' section with checkboxes for 'Event level', 'Event date & time', 'Device target', and 'Event notice'. A 'Remark' text area is also present. At the bottom right of the settings area is an 'Apply' button. At the very bottom of the page are 'OK' and 'Cancel' buttons. The footer contains the text 'Copyright©2014 D-Link Corporation.'

CWM Configuration

Monitor


Event

Condition

Condition Manager

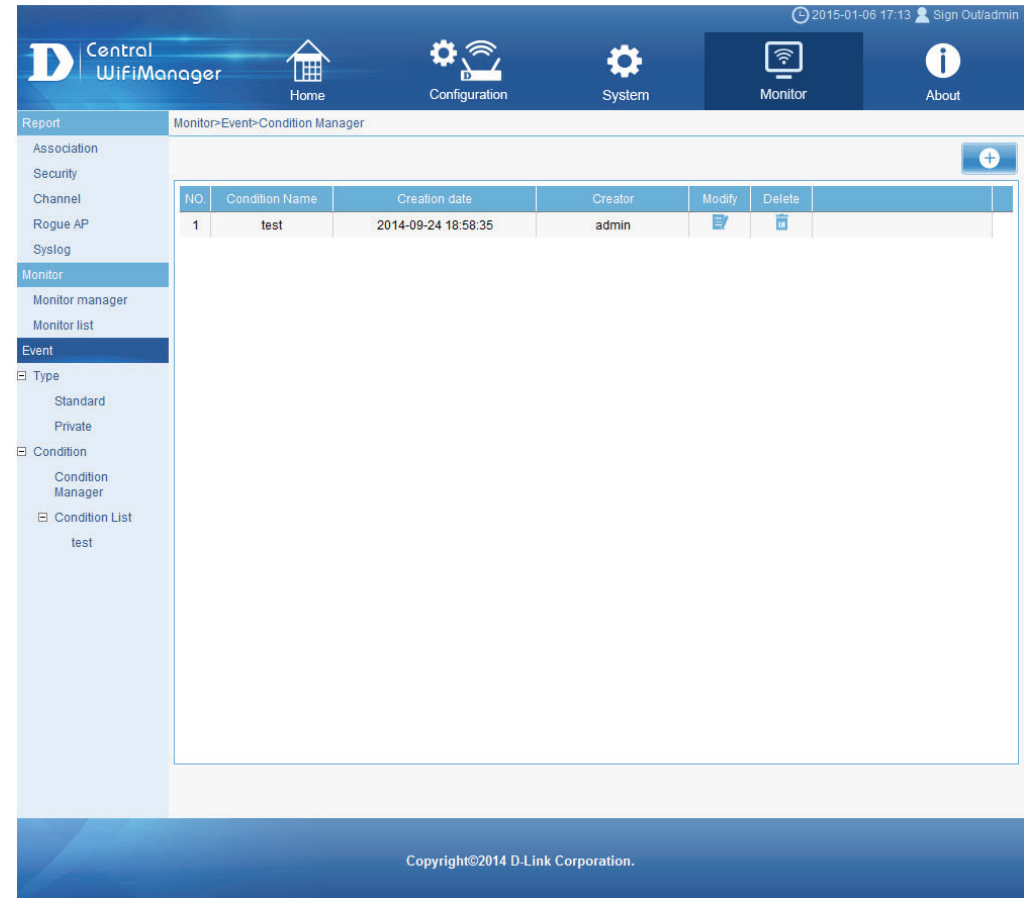
After clicking on **Monitor** in the top panel and **Event > Condition > Condition Manager** in the left panel, the following page will be displayed. On this page we can view, create and configure watch manager profiles.

Existing Condition Manager profiles are displayed in the table on this page.



Click the  button to create a new Condition Manager profile.

Click the  icon to modify an existing Condition Manager profile.

Click the  icon to delete an existing Condition Manager profile.



The screenshot shows the Central WifiManager web interface. The top header includes the logo, navigation icons for Home, Configuration, System, Monitor, and About, and a user profile section with 'Sign Out/admin' and the date '2015-01-06 17:13'. The left sidebar contains a navigation menu with categories: Report, Monitor, Event, and Condition. The 'Event' category is expanded, showing 'Type' (Standard, Private), 'Condition' (Condition Manager), and 'Condition List' (test). The main content area displays a table with the following data:

NO.	Condition Name	Creation date	Creator	Modify	Delete
1	test	2014-09-24 18:58:35	admin		

At the bottom of the page, there is a copyright notice: Copyright©2014 D-Link Corporation.

CWM Configuration

Monitor

Event

Condition

Condition Manager

Create Condition

After clicking the  button, the following page will be available. On this page we can create a new condition manager profile.

The following parameters can be configured:

Parameter	Description
Name	Enter the condition manager profile's name here.
Event List	To add an event to the event list, click on the Add button. To remove an event from the event list, select it and click on the Delete button.
Device List	To add a device to the device list, click on the Add button. To remove a device from the device list, select it and click on the Delete button.

Click the **OK** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

Central WifiManager

Home Configuration System Monitor About

Report Monitor>Event>Condition Manager >Create Watch

Association Security Channel Rogue AP Syslog Monitor Monitor manager Monitor list Event Type Condition Condition Manager Condition List test

Name: Maximum number of characters allowed is 50.

Event list

Device list

Copyright©2014 D-Link Corporation.

CWM Configuration

Monitor

Event

Condition

Condition Manager

Create Condition

After clicking the **Add** button next to the **Event List** parameter, the following window will appear.

In the **All Event** section, all available trap events will be displayed.

To use one or more of these events, select them and click on the **>>** button add them to the **Selected Event** section.

To remove one or more of the selected events from the **Selected Events** section, select them and click on the **<<** button.

Click the **OK** button to accept the selections made.

Click the **Cancel** button to discard the selections made and return to the previous page.

Copyright©2014 D-Link Corporation.

CWM Configuration

Monitor

Event

Condition

Condition Manager

Create Condition

After clicking the **Add** button next to the **Device List** parameter, the following window will appear.

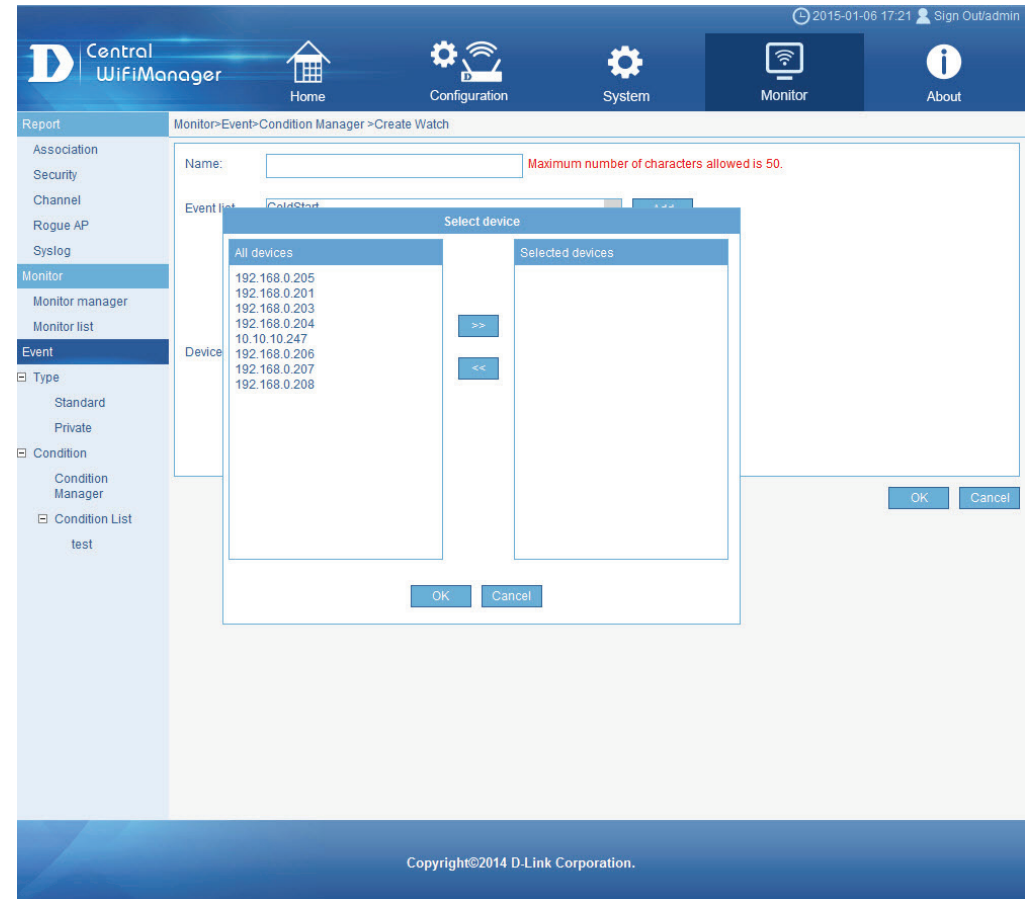
In the **All Device** section, all available access points in the network, managed by this application, will be displayed.

To use one or more of these devices, select them and click on the **>>** button add them to the **Selected Devices** section.

To remove one or more of the selected devices from the **Selected Devices** section, select them and click on the **<<** button.

Click the **OK** button to accept the selections made.

Click the **Cancel** button to discard the selections made and return to the previous page.




CWM Configuration | Monitor | Event | Condition | **Condition List**

After creating watch manager profiles in the previous section, those profiles will be available for selection under the **Condition List** option in the left panel. In this example, we created a Condition manager profile called **WiFi-Link-Down** that will generate events when an access point in this network's wireless link goes down. After clicking on **Monitor** in the top panel and **Event > Condition > Condition List > WiFi-Link-Down** in the left panel, the following page will be displayed. On this page we can view watch list messages that were generated based on the watch manager profile's settings.


To filter the messages displayed in this table, the following parameters can be configured:

Parameter	Description
Date	Select the starting date by clicking in the first text box available and select the starting date from the option available. Do the same for the ending date selection in the second text box.
Event Level	Select the event level from the drop-down list provided. Options to choose from are all , critic , error , warning , and notice .
Node IP	Enter the node's IP address here.
Keyword	To display only entries that contain a certain keyword, enter that keyword in this text box.


Click the  button to display only the entries based on the criteria entered.

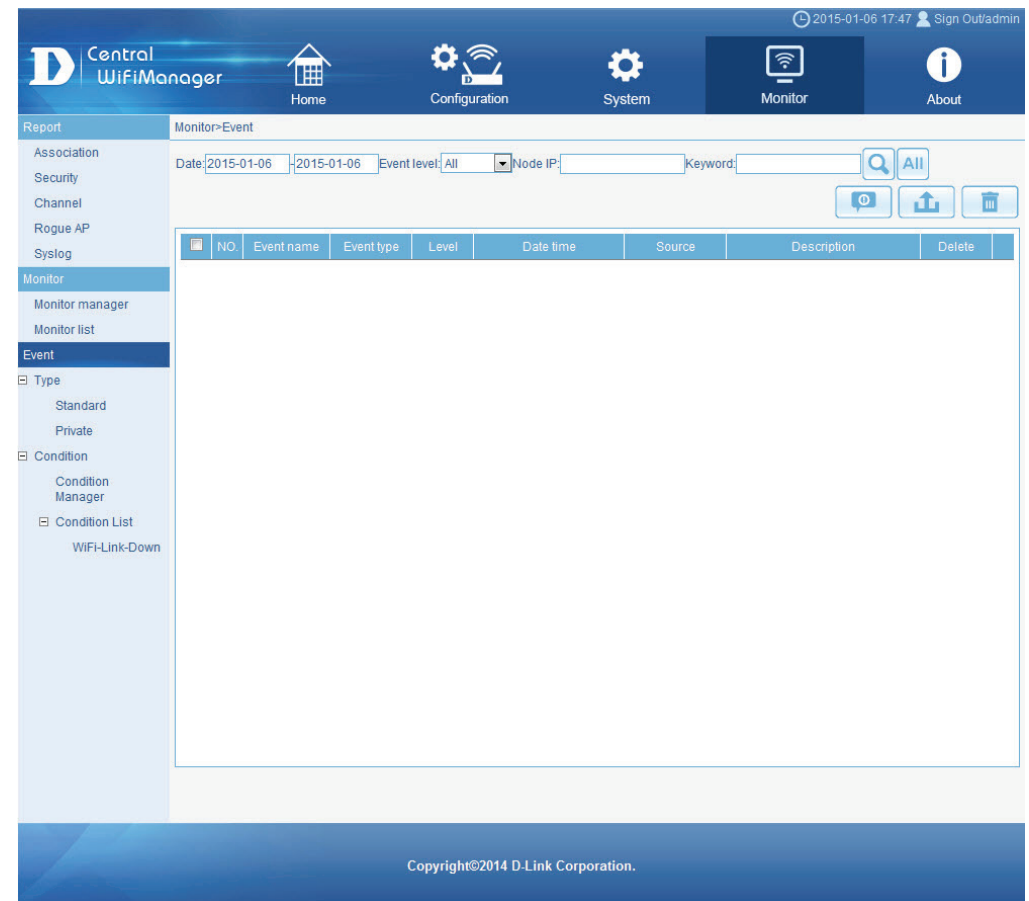
Click the  button to display all private events that have taken place.

Click the  button to create a new event and notice.

Click the  button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

Click the big  button to remove all entries from the event table.

Click the small  button next to a specific entry to remove only that entry from the event table.



The screenshot shows the Central WifiManager web interface. The top navigation bar includes the D-Link logo, the title 'Central WifiManager', and several icons for Home, Configuration, System, Monitor, and About. The user is logged in as 'admin' on '2015-01-06 17:47'. The left sidebar menu is expanded to the 'Event' section, with 'Condition List' selected. The main content area is titled 'Monitor-Event' and contains a search and filter section with fields for Date (2015-01-06 to 2015-01-06), Event level (All), Node IP, and Keyword. Below this is a table with columns: NO, Event name, Event type, Level, Date time, Source, Description, and Delete. The table is currently empty. At the bottom of the page, there is a copyright notice: 'Copyright©2014 D-Link Corporation.'

CWM Configuration

Monitor

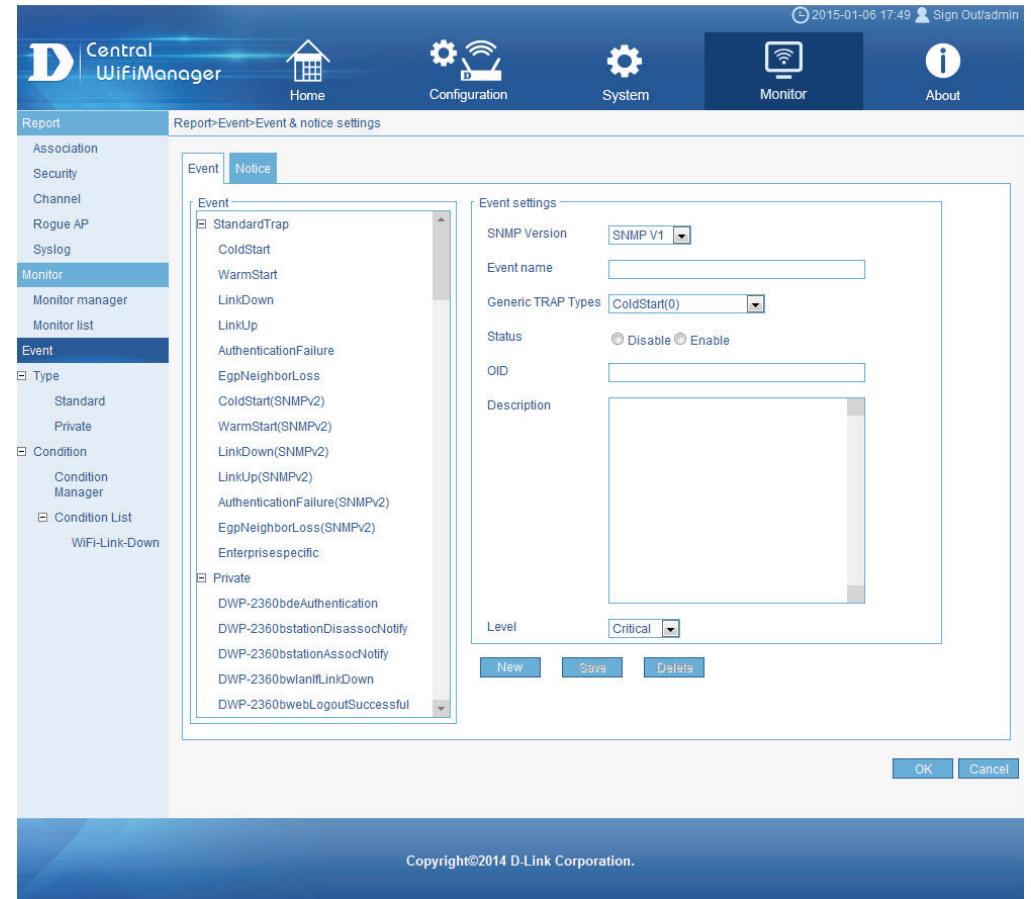
Event

Condition

Condition List

To create or configure standard SNMP event and notice settings, refer to “**Standard**” on page 85.

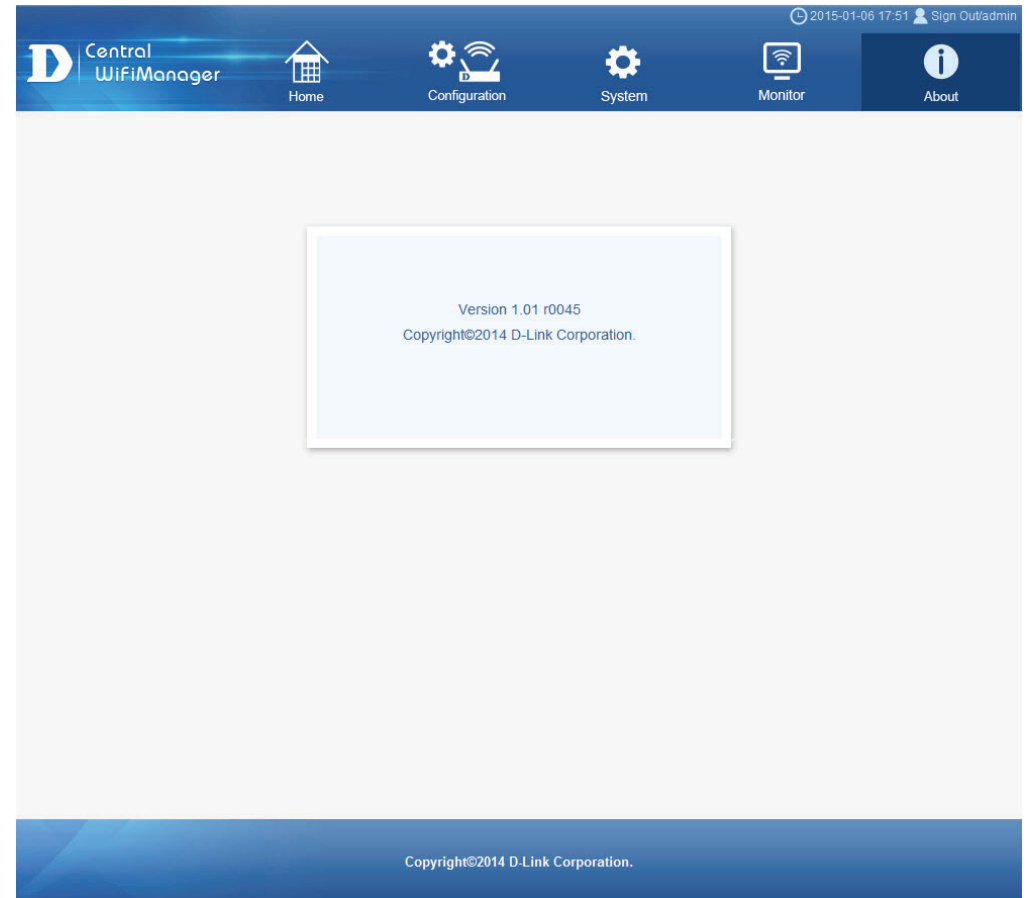
To create or configure private SNMP event and notice settings, refer to “**Private**” on page 88.



CWM Configuration

About


After clicking on **About** in the top panel, the following page will be displayed. On this page we can view the version number and copyright notice of the Central WifiManager Server application.

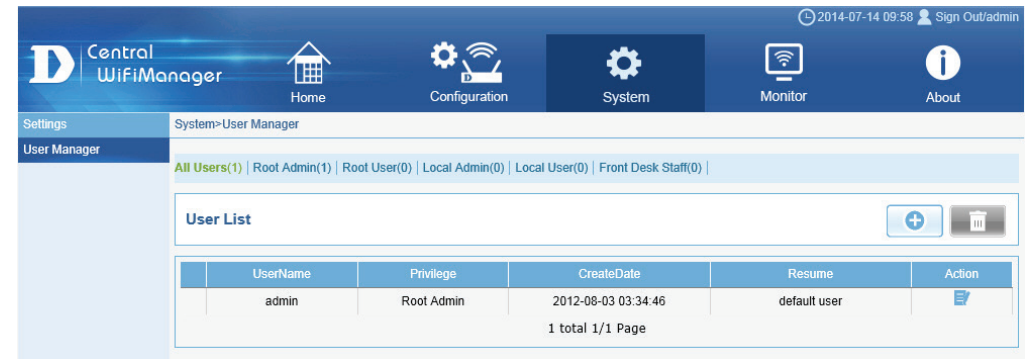



Appendix A - Front Desk Staff & User Access

Front desk user accounts can be created to allow guests to use the wireless network for a limited amount of time. Normally, restricted wireless access is given to front desk wireless users. In this section we'll discuss how to create and use a front desk staff account and how generate guest pass codes.

To setup a **front desk staff** account, we need to enter the Central WifiManager Server application with an administrative account. Navigate to **System**, in the top menu, and **User Manager**, in the left menu.

Click the  button, to create a new user account.



After clicking the  button, the following page will be available. The following parameters can be configured:

Parameter	Description
Username	Enter the front desk staff account's username here.
Password	Enter the front desk staff account's password here.
Privilege	Select the Front Desk Staff option here.
E-mail	Enter the front desk staff person's email address here.
Description	Enter additional information about this account here.

Click the **OK** button to create the new account.

Click the **Reset** button to clear out the information entered in the fields.

The screenshot shows the 'System>User manager' configuration page. It has the same navigation and breadcrumb as the previous screenshot. The form contains the following fields:

- Username:** A text input field with a red asterisk and a red note 'Maximum length: 64 characters'.
- Password:** A text input field with a red asterisk.
- Privilege:** A dropdown menu currently showing 'Root admin'.
- E-mail:** A text input field.
- Description:** A large text area with a red note 'Maximum length: 50 characters' at the bottom.

At the bottom right of the form are three buttons: 'OK', 'Reset', and 'Cancel'.

Appendix A - Front Desk Staff & User Access

After successfully adding the front desk staff account, it will be displayed in the user manager table.

	UserName	Privilege	CreateDate	Resume	Action
	admin	Root Admin	2012-08-03 03:34:46	default user	
<input type="checkbox"/>	front	Front Desk Staff	2014-07-14 10:09:11	Additional resume information placed here.	

In the next step we need configure our guest wireless network to use pass codes for user authentication. Navigate to **Configuration**, in the top menu, and select your network, in the left menu. In our example, the guest network is located within the **Server-Room** network, at the **Headquarters** site.

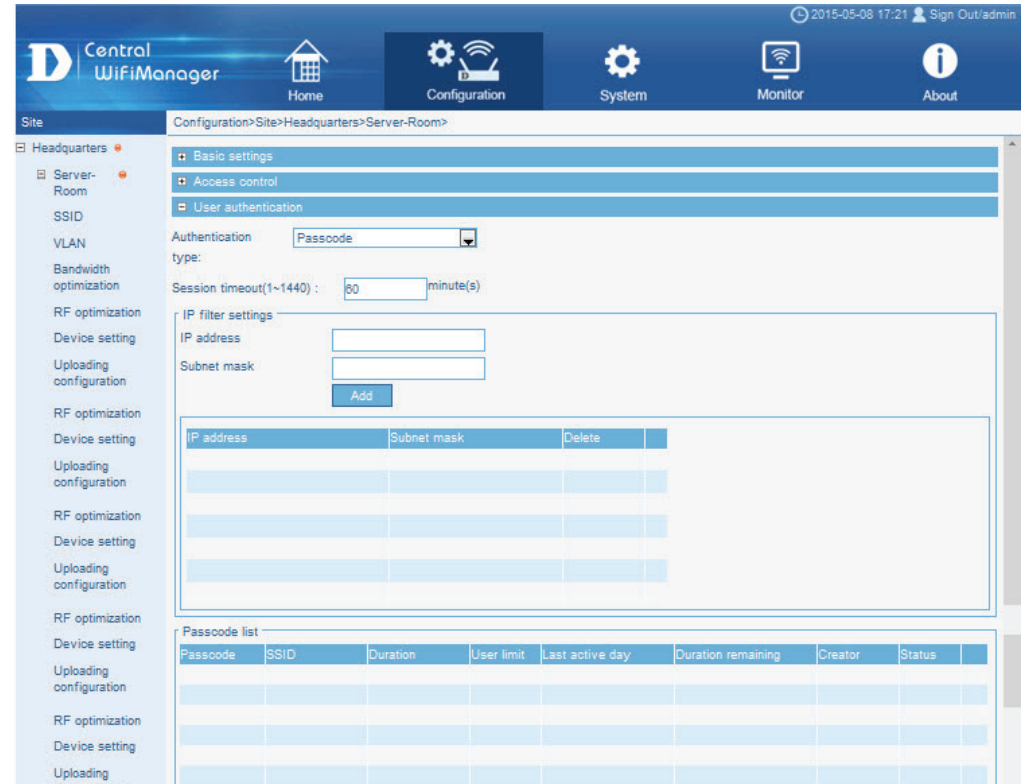
In this example, the guest network's SSID is called **SR-Guest**. To enable pass code user authentication for this SSID, click the button in the **SR-Guest** entry to modify the SSID.

Index	SSID	Band	Security	Access control	User authentication	Modify	Delete
Primary	SR-WIFI	2.4GHz	Open System	Disable	Disable		
SSID1	SR-Guest	2.4GHz	Open System	Disable	Disable		

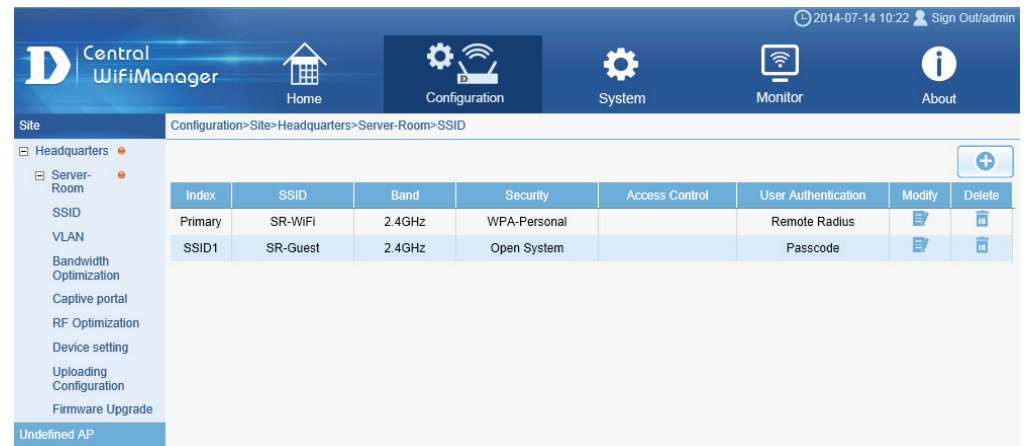
Appendix A - Front Desk Staff & User Access

After clicking the  button, the following page will be available. Here we can modify the parameters of the SSID called **SR-Guest**.

In the **User Authentication** section, select **Passcode** as the **Authentication Type** and click the **Save** button to accept the changes made.



After successfully modifying the SSID to use pass codes for user authentication, the **User Authentication** entry column should display **Passcode** for the **SR-Guest** entry.

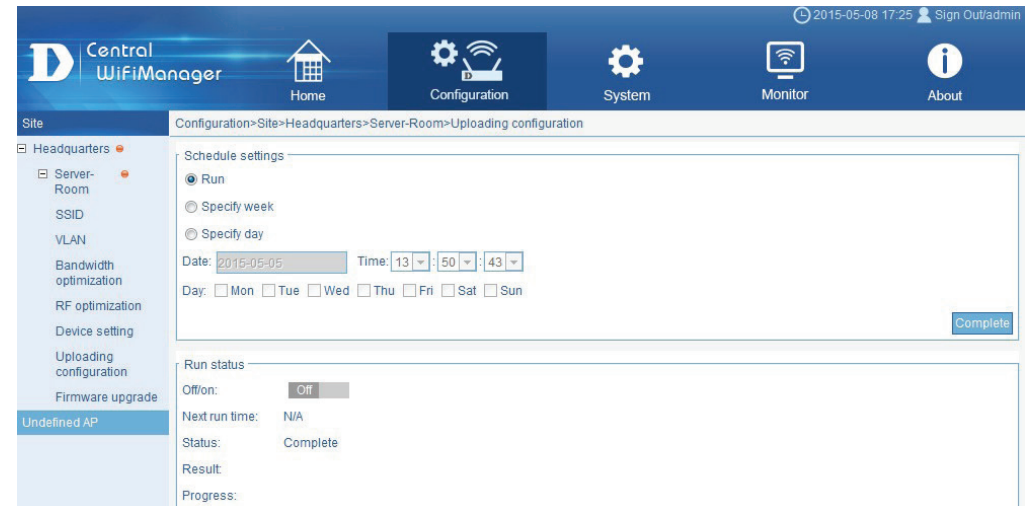


Appendix A - Front Desk Staff & User Access

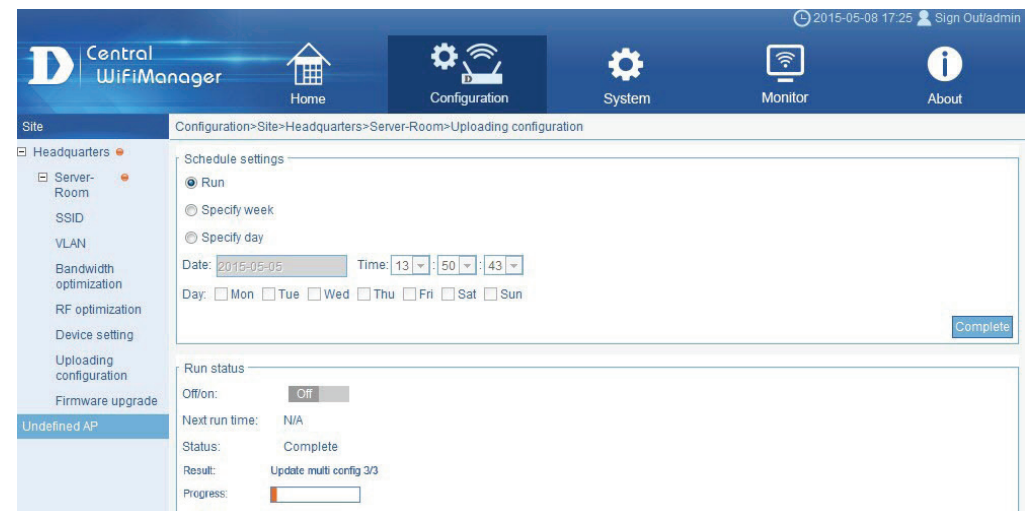
Access points in the network, will not know about these new changes until the configuration of the relevant access points have been updated. To manually update the configuration of the relevant access points, navigate to **Configuration**, in the top menu, and your network link in the left menu. The network in this example is **Server-Room**.

Select the **Upload Configuration** option in the left menu. In the **Schedule Settings** section, select the **Run** option and click the **Complete** button.

The configuration will now be uploaded to the relevant access points as displayed in the **Run Status** section.



The screenshot shows the Central WiFiManager interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar lists various configuration options, with 'Upload configuration' highlighted. The main content area is titled 'Configuration > Site > Headquarters > Server-Room > Uploading configuration'. Under 'Schedule settings', the 'Run' radio button is selected. The date is set to 2016-05-05 and the time to 13:50:43. A 'Complete' button is located at the bottom right of the 'Schedule settings' section. Below this, the 'Run status' section shows 'Off/on' as 'Off', 'Next run time' as 'N/A', and 'Status' as 'Complete'.




This screenshot is identical to the one above, showing the 'Upload Configuration' screen. However, the 'Run status' section now displays 'Result: Update multi config 3/3' and a progress bar, indicating that the configuration upload is in progress or completed.

Appendix A - Front Desk Staff & User Access




After the configuration file was uploaded to the access points, the **Status** option in the **Run Status** section should show **Complete**.

The screenshot shows the Central WifiManager interface. The top navigation bar includes Home, Configuration, System, Monitor, and About. The left sidebar shows a tree view with 'Headquarters' expanded, and 'Server-Room' selected. The main content area is titled 'Configuration>Site>Headquarters>Server-Room>Uploading configuration'. It features 'Schedule settings' with radio buttons for 'Run' (selected), 'Specify week', and 'Specify day'. Below this are date and time pickers. A 'Run status' section shows 'Off/on' as 'Off', 'Next run time' as 'N/A', 'Status' as 'Complete', 'Result' as 'Complete(Some devices fail)', and 'Progress' as an empty bar. A 'Complete' button is visible in the bottom right of the main content area.


Next we need to add the new front desk staff user account to the site's network member list. Navigate to the Configuration, in the top menu, and select the relevant site in the left menu. In this example our site's name is **Headquarters**.

All networks will be displayed in the **Network List** table. In this example, our network is called **Server-Room**. Click the  button next to the entry, to modify this network.

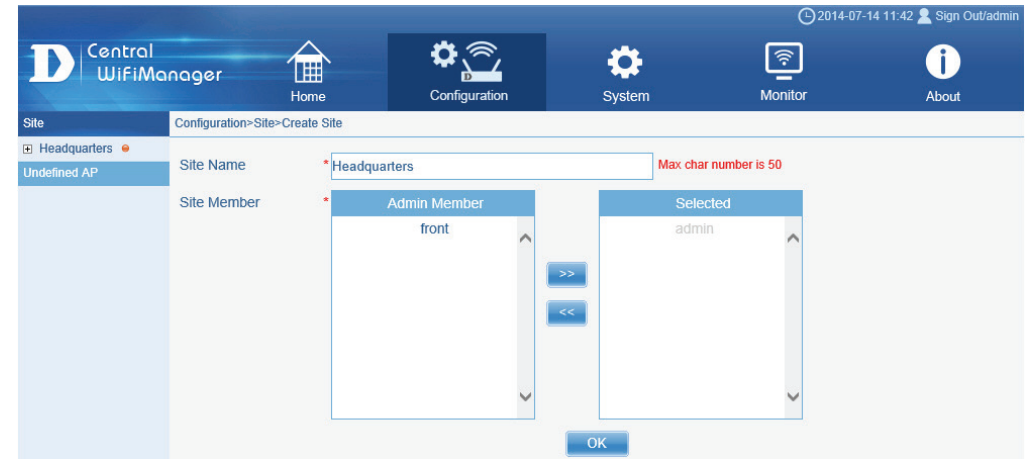
The screenshot shows the Central WifiManager interface. The top navigation bar includes Home, Configuration, System, Monitor, and About. The left sidebar shows a tree view with 'Headquarters' expanded, and 'Server-Room' selected. The main content area is titled 'Configuration>Site>Headquarters'. It features a 'Network List' table with the following data:

Network Name	Admin Member	Creator	Creat Date	Modify	Delete	Export
Server-Room	admin	admin	2014-07-01 12:23:01			

Appendix A - Front Desk Staff & User Access

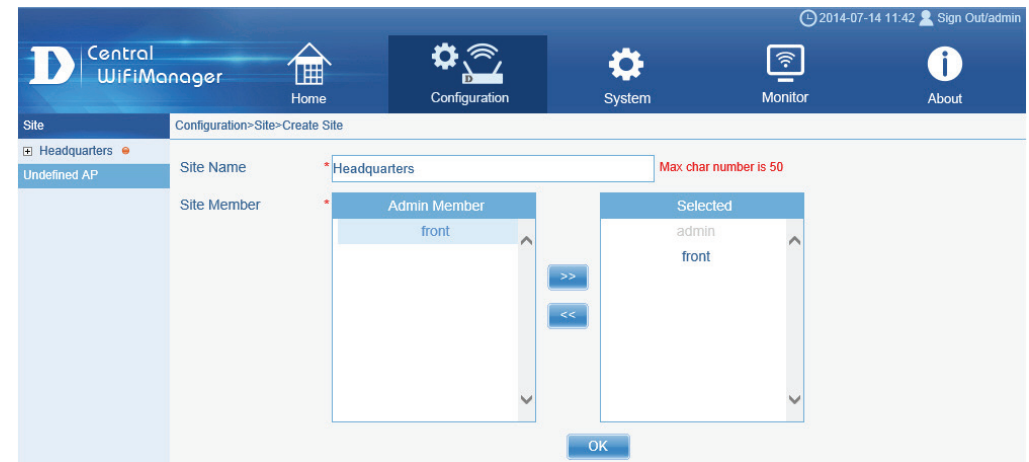
After clicking the  button, the following page will be available. The front desk staff user account will now be available and can be added to this network by selecting it and clicking on the >> button to move the account over to the **Selected** column.

Click the OK button to accept the changes made.



Click the **OK** button to accept the changes made.

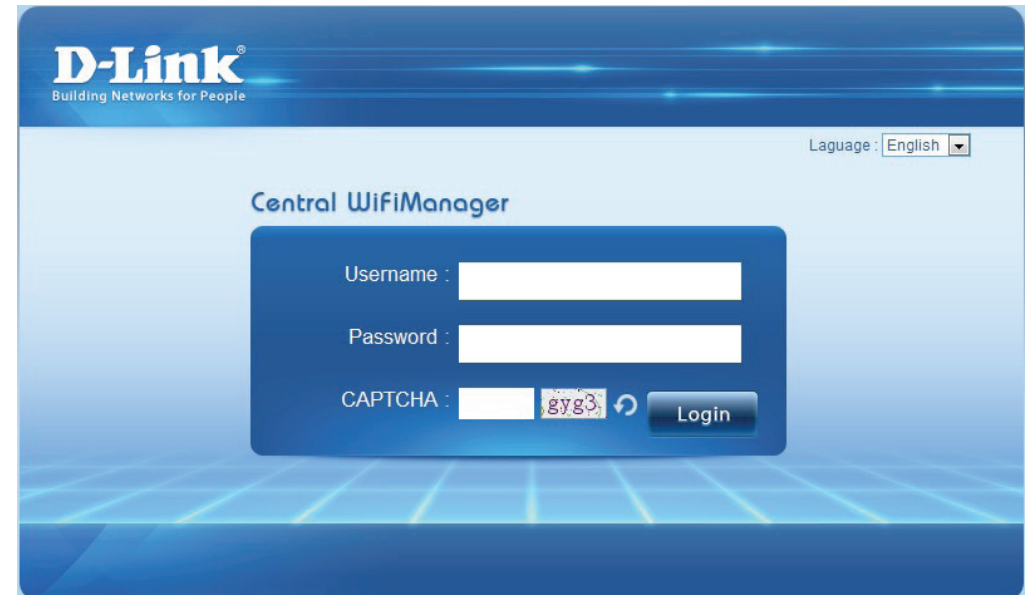
After this, upload the configuration files to the access points in the network again. Refer to the steps discussed earlier on how to do this.



Appendix A - Front Desk Staff & User Access

Now we can log out of the administrative account, and log back in with our front desk staff account.

Enter the front desk staff account's username and password in the spaces provided and click the **Login** button to enter the front desk staff account.



The screenshot shows the D-Link Central WifiManager login interface. At the top left is the D-Link logo with the tagline "Building Networks for People". In the top right corner, there is a language selection dropdown menu currently set to "English". The main heading "Central WifiManager" is centered above a dark blue login form. The form contains three input fields: "Username", "Password", and "CAPTCHA". The CAPTCHA field displays the characters "8Yg3" and includes a refresh icon. A "Login" button is positioned to the right of the CAPTCHA field.

Appendix A - Front Desk Staff & User Access

After successfully logged in, using the front desk staff account, the following page will be available. On this page we can generate a pass code for front desk users.

The following parameters can be configured:

Parameter	Description
SSID	The network SSID will be displayed that front desk user can use to temporarily access the wireless network using the pass code that will be generated here.
Security Key	A pass code can be manually entered here. Leave this field blank to allow the system to generate a random pass code. Select the Display Security Key option to display the letter typed into this field.
Pass Code Quantity	Enter the amount of pass codes that will be generated here. Normally we'll only generate one pass code.
Duration	Enter the duration for this wireless connection here. This value must be in hours.
Last Active Day	Select the last active date that this code can be used here.
Device Limit	Enter the device limit value here. This is the maximum amount of active users that can use this pass code.


The screenshot shows the 'Central WifiManager' interface. The top navigation bar includes the logo and the text 'Central WifiManager'. The breadcrumb trail is 'Frontdesk>D-Link_HQ>PP>Generate passcode'. The left sidebar contains a menu with 'Generate passcode' selected. The main content area is titled 'Passcode settings' and contains the following fields:

- Band:** 2.4G (dropdown menu with a checked box for '2.4G & 5G')
- SSID:** GO to CWM24&Go to C
- Security key:** (text input field) with a checkbox for 'Display security key'.
- Passcode quantity:** (text input field)
- Duration:** (text input field) with a label 'Hours'.
- Last active day:** 2015-01-06
- User limit:** (text input field)

Click the **Generate** button to generate the new pass code.

Appendix A - Front Desk Staff & User Access

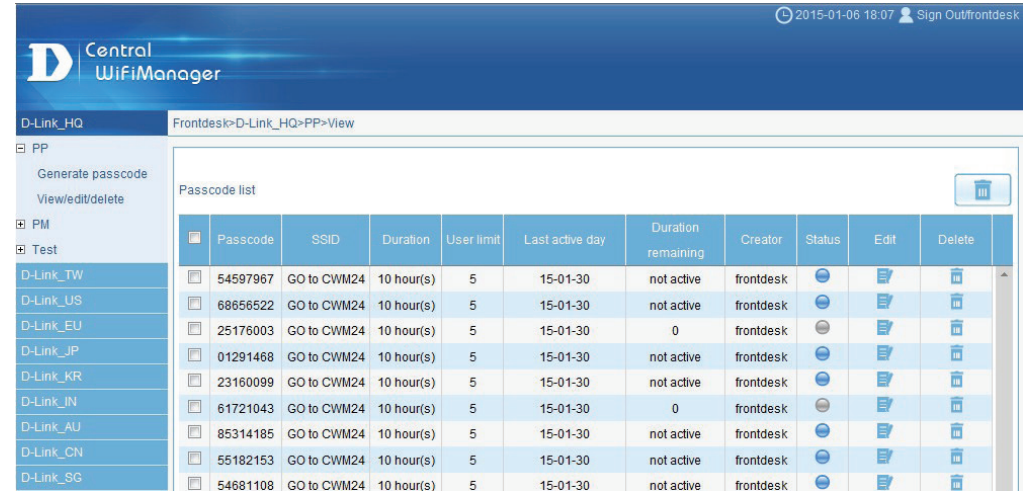
After clicking on the **View/Edit/Delete** option in the left menu, we can view the list of pass codes that was generated. Also the **Duration Remaining** and **Status** fields are displayed here, that are useful for front desk staff to monitor active and passive connections.

Click the  icon to modify an existing entry.

Click the  icon to delete an existing entry.

Pass codes can now be given to front desk users by front desk staff.

To generate new codes, front desk staff simply login to the Central WifiManager Server application, using the front desk staff user account details, enter the relevant ticket (pass code) information and click on the **Generate** button to get a code and give the code to the front desk user. Based on the **Duration** time specified, the ticket will expire and the entry can be removed.



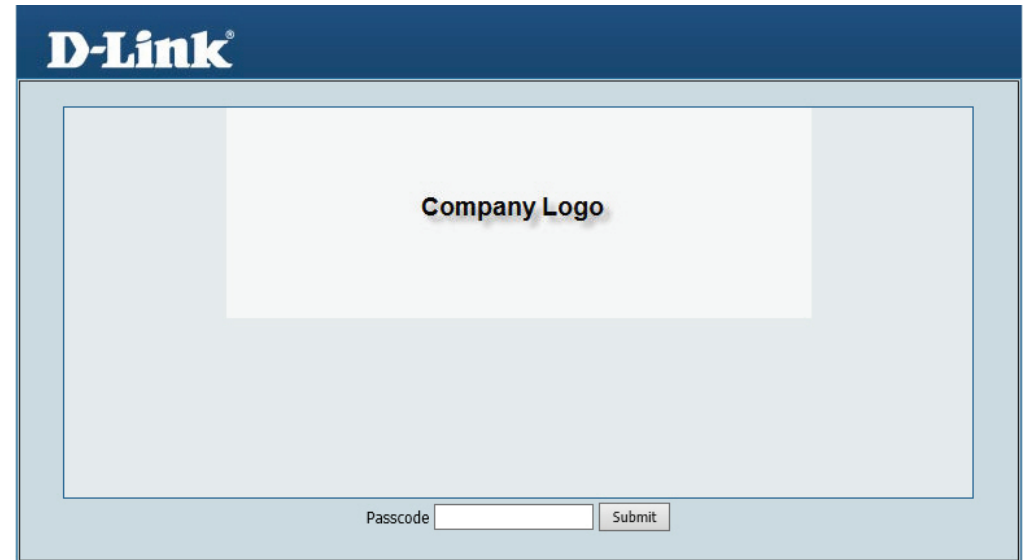
The screenshot shows the Central WifiManager interface. The top navigation bar includes the logo, the text "Central WifiManager", and a user profile section with the date "2015-01-06 18:07" and a "Sign Out/frontdesk" link. The main content area is titled "Frontdesk>D-Link_HQ>PP>View". On the left, there is a sidebar menu with options: "PP" (selected), "Generate passcode", "View/edit/delete", "PM", and "Test". The main area displays a "Passcode list" table with the following columns: Passcode, SSID, Duration, User limit, Last active day, Duration remaining, Creator, Status, Edit, and Delete. The table contains 10 rows of data, all generated by "frontdesk" and associated with "GO to CWM24".

Passcode	SSID	Duration	User limit	Last active day	Duration remaining	Creator	Status	Edit	Delete
54597967	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		
68656522	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		
25176003	GO to CWM24	10 hour(s)	5	15-01-30	0	frontdesk	not active		
01291468	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		
23160099	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		
61721043	GO to CWM24	10 hour(s)	5	15-01-30	0	frontdesk	not active		
85314185	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		
55182153	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		
54681108	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk	not active		

Appendix A - Front Desk Staff & User Access

Front desk users simply connect to the wireless network available and when trying to connect to the network or Internet, using their Web browser, users will be asked to enter the pass code.

After entering the correct code, supplied by front desk staff, front desk users can connect to the network or Internet for the duration of the ticket.



The screenshot displays the D-Link login interface. At the top left, the **D-Link** logo is visible. The main content area features a large, light-colored rectangular box with the text **Company Logo** centered inside. Below this box, there is a label **Passcode** followed by a text input field and a **Submit** button.

Appendix B - How to customize Captive Portal Login Page

There are three styling options provided for customizing the look and feel of the captive portal login page. Please follow instructions below for a successful customization of the login page.

Each styling option represents different UI style; customization for any option is done by editing its web page source files. Below is a quick overview for files that can be edited as they vary for each styling option:

- **Pages_default:** Provides options to customize the text and images shown on the login page
- **Pages_license:** Provides options to customize the text and images shown on the login page, including the ability to place your own logo image.
- **Pages_headerpic:** Provides options to customize the text and images shown on the login page, including the ability to place your own logo image and a header image at the top of the page.

Image is customized by replacing the existing image files. Text is customized by editing the “text.js” file.

Obtaining the source files

You can obtain the source file by going to the “SSID” page under the “Configuration” menu.

In “Splash page customization”, select the style from the drop-down menu and click on “Download Template” to download its source file.

You should see the downloaded source file with the same name as the one from the drop-down menu. The file will be compressed with the extension of “.tar” (eg. Pages_default.tar). Please use a file compression tool such as 7zip or winrar to decompress the file. The source files should then be located in an extracted folder.

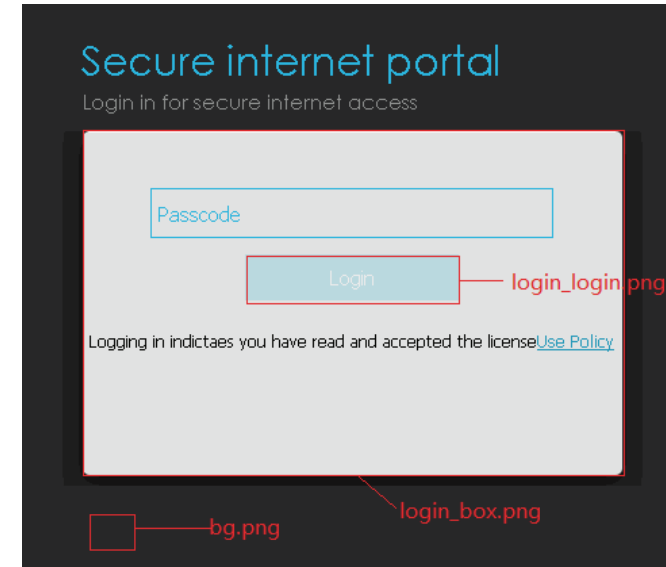
The screenshot shows the Central WifiManager configuration interface. The top navigation bar includes 'Home', 'Configuration', 'System', 'Monitor', and 'About'. The left sidebar shows a tree view with 'SS' expanded, containing 'NN', 'SSID', 'VLAN', 'Bandwidth optimization', 'RF optimization', 'Device setting', 'Uploading configuration', and 'Firmware upgrade'. The main content area is titled 'Configuration>Site>SS>NN>SSID'. It features a 'Passcode list' table with columns: Passcode, SSID, Duration, User limit, Last active day, Duration remaining, Creator, and Status. Below the table, there are sections for 'Web redirection' (with a checkbox and a 'Website' input field), 'Splash page customization' (with a 'Choose template' dropdown set to 'pages_default', 'Preview', 'Upload login file', 'Delete the style', and 'DownLoad Template' buttons), and 'Enable white list' (with a checkbox, 'MAC address' input, 'Add' button, 'Upload white list file' input, 'Browse...' button, and 'Upload' button). A table at the bottom has columns 'No.', 'MAC address', and 'Delete'.

Appendix B - How to customize Captive Portal Login Page

Contents and illustrations of each styling source files

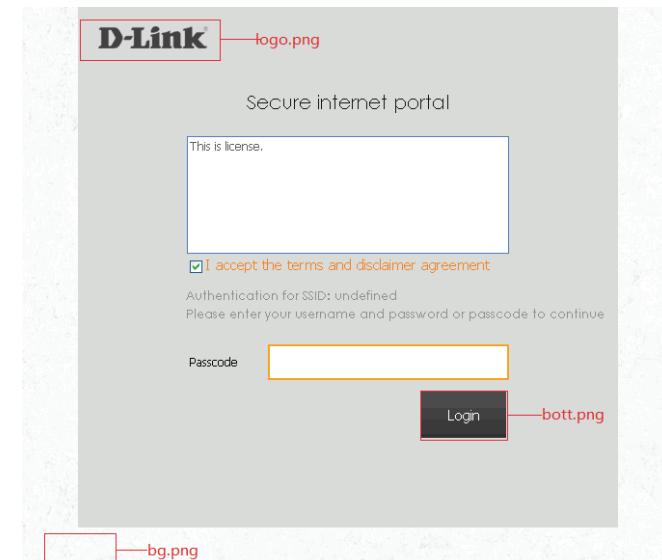
Pages_default: bg.png, login_box.png, login_login.png, text.js

- Please make sure to use png image files and remain using the same file names for your customization.
- Please make sure UTF-8 encoding for texts entered in the text.js file.



Pages_license: bg.png, bott.png, logo.png, text.js

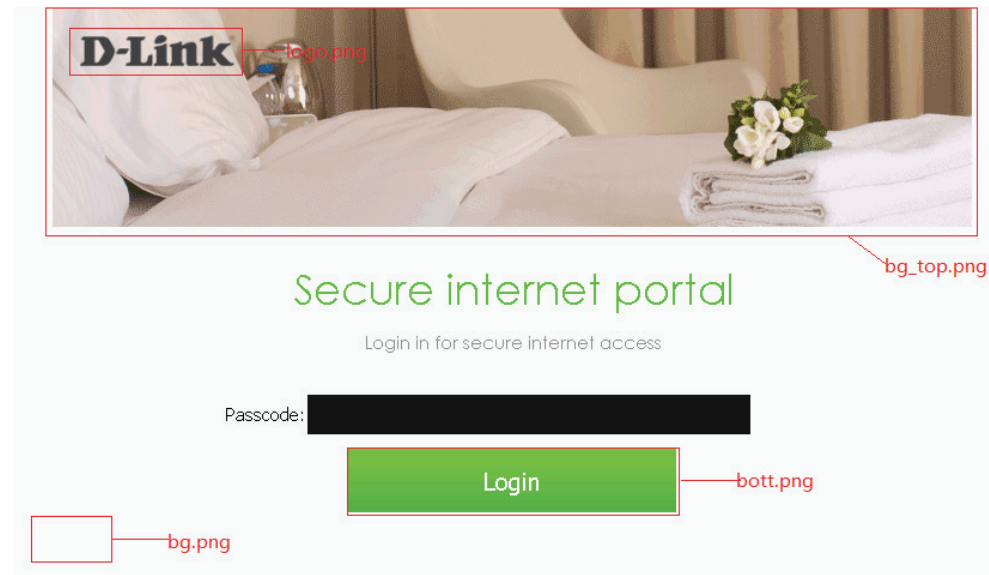
- Please make sure to use png image files and remain using the same file names for your customization.
- Please make sure UTF-8 encoding for texts entered in the text.js file.



Appendix B - How to customize Captive Portal Login Page

Pages_headerpic: bg.png, bg_top.png, bott.png, logo.png, text.js

- Please make sure to use png image files and remain using the same file names for your customization.
- Please make sure UTF-8 encoding for texts entered in the text.js file.



Editing texts in the text.js file

Open the text.js with text editor software. Locate the following parameters in the file and change their values to after the "=" to customize texts shown in the login page:

```
var username="Username";  
var password="Password";  
var login="Login";  
var license_notice="Logging in indicates you have read and accepted the license";  
var license_link="Use Policy";
```

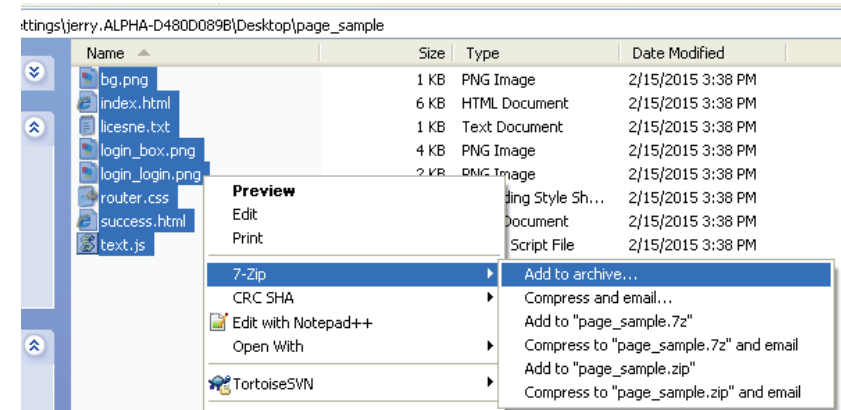
Appendix B - How to customize Captive Portal Login Page

Uploading the source file after customization

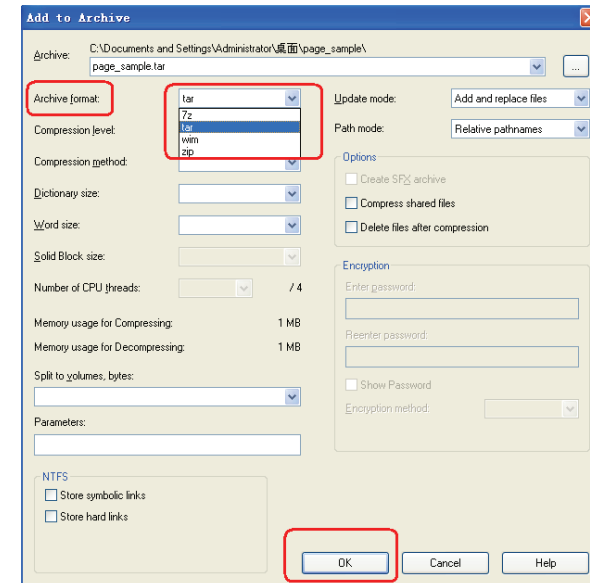
After you are done editing the extracted source files, you would need to compress the files back to a “.tar” file before uploading it back the CWM.

Below is an example to compress the files using 7zip:

1. Select all the extracted source files and right-click. From the drop-down menu, select “7-Zip” >> “Add to archive”

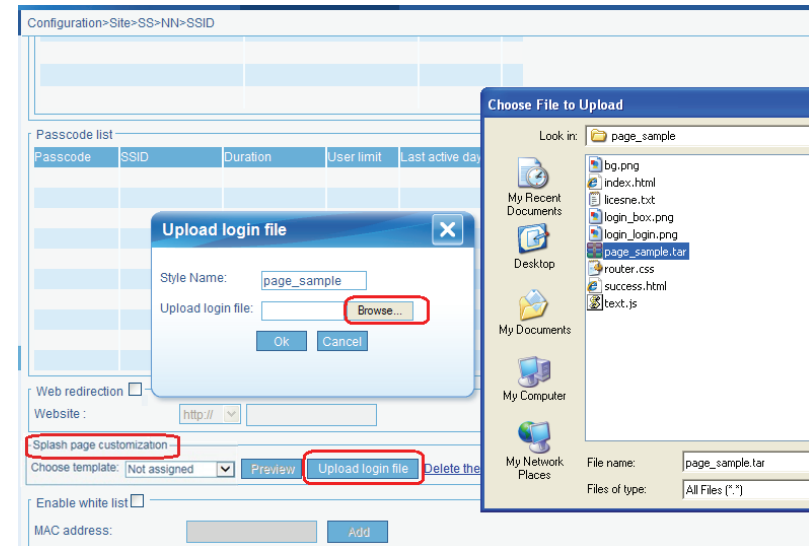


2. In the dialog, select “tar” as the archive format from the drop-down menu shown below and click “OK” to finish. (*Please make sure the compressed file does not exceed 448KB. Exceeding the size limit will result in a failed upload)



Appendix B - How to customize Captive Portal Login Page

3. In the CWM web management UI, go to “Configuration” >> “SSID”. Under “Splash page customization”, click “Upload login file”. A dialog should be displayed to allow you to add a new style profile. Enter a desired name and click “Browse”, this should open another dialog which allows you to locate the source file for upload.



4. After uploading the source file successfully, the new style should be available from the drop-down menu, which you can select and finish configuration for captive portal login page customization.

